PLAN DU SOUS SAVOIR S33

A. Architecture des réseaux locaux (modèle hiérarchique)

I. Modèle de réseau hiérarchique :

La conception de réseau hiérarchique implique la division du réseau en couches distinctes. Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global.
Le modèle de conception hiérarchique classique se divise en trois couches : la couche d'accès, la couche de distribution et la couche cœur de réseau.

- La couche accès permet aux utilisateurs répartis dans les groupes de travail d'accéder au réseau.
- La couche distribution assure une connectivité basée sur les politiques d'administration et de sécurité.
- La couche cœur de réseau ou principale assure l'optimisation du transport entre les sites. Cette couche est souvent appelée backbone.

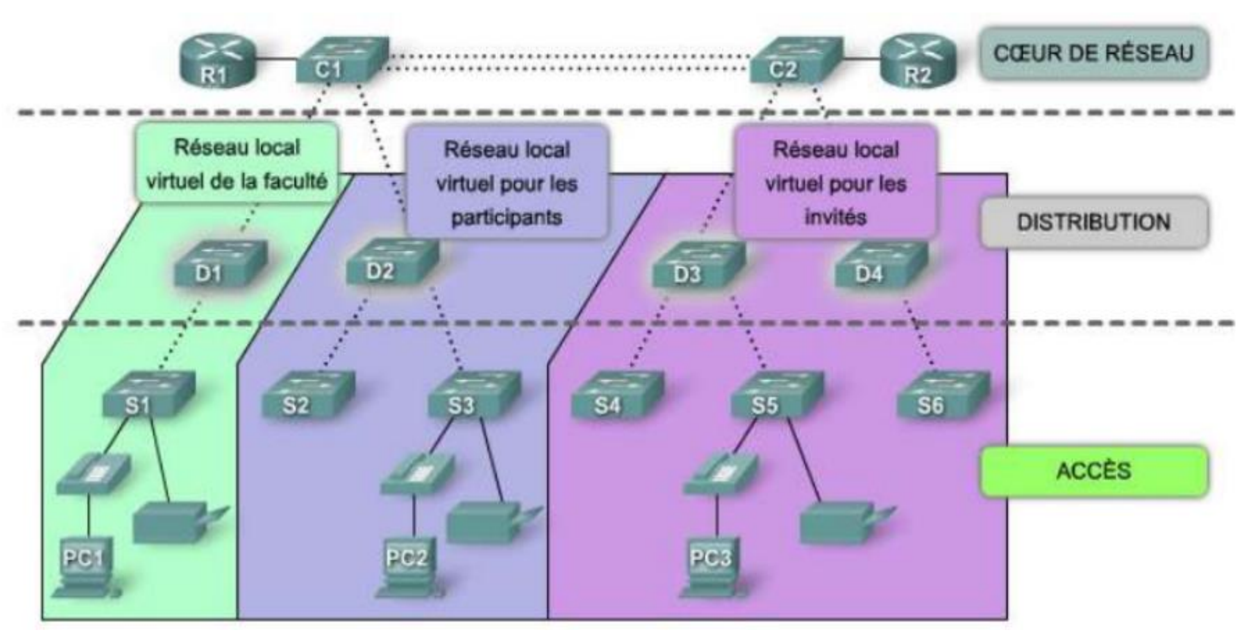


Fig 1 : modèle de réseau hiérarchique

L'utilisation d'un modèle de conception hiérarchique permettra d'apporter plus facilement des modifications au réseau au fur et à mesure de la croissance de l'organisation.

1.1. Vue d'ensemble de la couche accès :

La couche accès est le point d'entrée au réseau pour les stations de travail des utilisateurs, les imprimantes et les serveurs.

- **Fonctions :**
  - Bande passante partagée
  - Bande passante réservée
  - Filtrage de la couche MAC
  - Micro segmentation

- **Commutateurs de la couche accès**

Les commutateurs de la couche accès fonctionnent au niveau de la couche 2 du modèle OSI et fournissent des services tels que l'appartenance au VLAN. Le commutateur de couche accès a pour principal objectif d'autoriser l'accès des utilisateurs finaux sur le réseau.
Ces commutateurs ont les caractéristiques suivantes :
  - faible coût
  - une densité de port élevée

- **Exemples de commutateurs de la couche accès**
  - Gamme Catalyst 1900
  - Gamme Catalyst 2820
  - Gamme Catalyst 2950
  - Gamme Catalyst 4000
  - Gamme Catalyst 5000



Gamme Catalyst 4000

1.2. Vue d'ensemble de la couche distribution

Elle a pour rôle de définir les limites à l'intérieur desquelles le traitement des paquets peut avoir lieu. Elle segmente également les réseaux en domaines de broadcast. Des politiques de traitement peuvent être appliquées et des listes de contrôle d'accès peuvent filtrer les paquets. Les commutateurs de cette couche fonctionnent au niveau de la couche 2 et de la couche 3

- **Fonctions :**
  - le regroupement des connexions du local technique,
  - la définition des domaines de broadcast et de diffusion multipoint (multicast),
  - le routage des LAN virtuels (VLAN),
  - le changement de média si nécessaire,
  - la sécurité.

- **Commutateurs de la couche distribution**

Les commutateurs de la couche distribution sont les points de regroupement de plusieurs commutateurs de la couche accès. Le commutateur doit être en mesure de supporter la totalité du trafic des équipements de la couche accès.
Ces commutateurs ont les caractéristiques suivantes :

  - performances élevées
  - «commutateurs multicouches» combinent en un seul équipement les fonctions d'un routeur et d'un commutateur.

- **Exemples de commutateurs de la couche distribution**
  - Catalyst 2926G
  - Catalyst 3550
  - Gamme Catalyst 5000
  - Gamme Catalyst 6000



Gamme Catalyst 6000

1.3. Vue d'ensemble de la couche principale

La couche principale est un backbone de commutation à haut débit.

- **Fonctions :**
  - Cette couche du réseau ne doit pas effectuer de tâches liées au traitement de paquets.
  - L'établissement d'une infrastructure principale avec des routes redondantes procure de la stabilité au réseau pour pallier une éventuelle défaillance d'un équipement
  - Des commutateurs ATM ou Ethernet peuvent être utilisés.

- **Commutateurs de la couche principale**

Les commutateurs de couche principale sont conçus pour fournir en cas de besoin une fonctionnalité de couche 3 efficace.

- **Exemples de commutateurs de la couche principale**
  - Gamme Catalyst 6500
  - Gamme Catalyst 8500
  - Gamme IGX 8400
  - Lightstream 1010



Lightstream 1010

1.4. Avantages d'un réseau hiérarchique :

Les conceptions de réseau hiérarchique présentent de nombreux avantages :

- Evolutivité : les réseaux hiérarchiques peuvent être aisément étendus.
- Redondance : la redondance au niveau des différentes couches permet de garantir la disponibilité de chemins d'accès.
- Performances : l'agrégation de liaisons entre les niveaux et les commutateurs des couches principales permet de bénéficier d'une vitesse proche de celle du câble à travers le réseau.
- Sécurité : la sécurité de port au niveau de l'accès et les stratégies au niveau de la distribution renforcent la sécurité du réseau.
- Facilité de gestion : la cohérence entre les commutateurs à chaque niveau simplifie davantage la gestion.
- Maintenance : la modularité de la conception hiérarchique permet une mise à l'échelle du réseau sans trop de complexité.

II. Principales caractéristiques d'un modèle de réseau hiérarchique :

La conception hiérarchique d'un réseau ne signifie pas qu'il ait été correctement conçu. Les caractéristiques suivantes vont nous aider à distinguer les bons des mauvais réseaux hiérarchiques.

2.1. Diamètre de réseau :

Le diamètre correspond généralement à une mesure de distance, mais dans ce cas, ce terme est utilisé pour mesurer le nombre de périphériques. Le diamètre de réseau correspond au nombre de périphériques que doit traverser un paquet avant d'atteindre sa destination. Lorsque vous maintenez un faible diamètre de réseau, cela garantit une latence faible et prévisible entre les périphériques

Le diamètre de réseau correspond au nombre de commutateurs dans le chemin d'accès du trafic entre deux points d'extrémité.

Fig 3 : Diamètre de réseau

2.2. Agrégation de bande passante :

L'agrégation de bande passante correspond à la prise en compte des exigences spécifiques de bande passante de chaque partie de la hiérarchie. Une fois les exigences de bande passante du réseau identifiées, des liaisons peuvent être agrégées entre des commutateurs spécifiques : il s'agit d'une agrégation de liaisons. L'agrégation de liaisons permet de combiner plusieurs liaisons de port d'un commutateur afin de bénéficier d'un débit plus élevé entre des commutateurs.

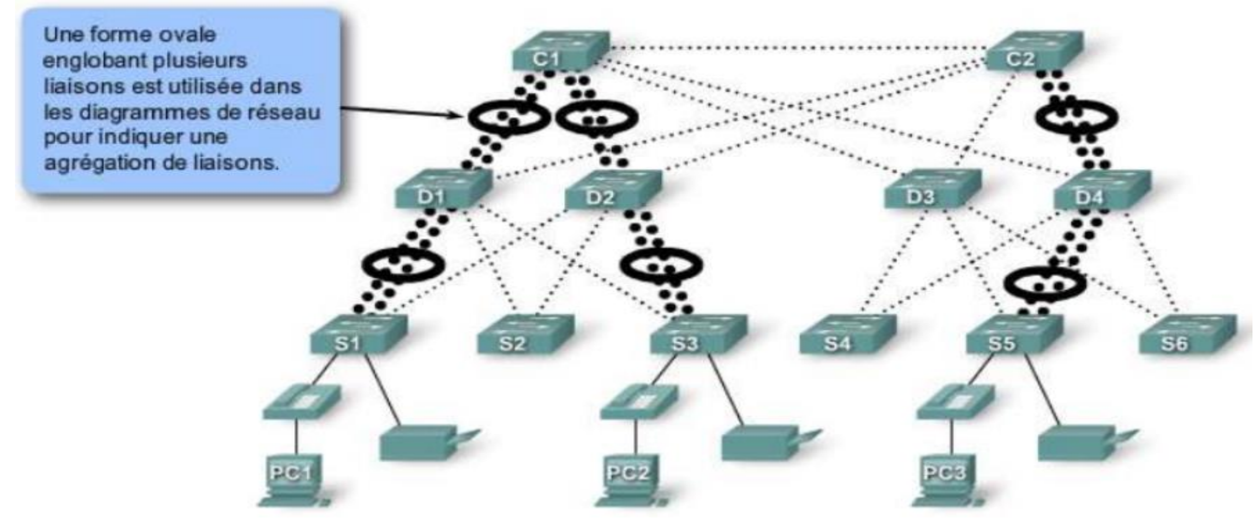


Fig 4 : Agrégation de bande passante

2.3. Redondance :

La redondance représente une partie de la création d'un réseau à disponibilité élevée. La redondance peut se présenter sous différentes formes. Par exemple, vous pouvez doubler les connexions réseau entre les périphériques, ou bien doubler les périphériques eux-mêmes.

Des réseaux modernes utilisent des liaisons redondantes entre des couches de réseau hiérarchique afin de garantir la disponibilité du réseau.

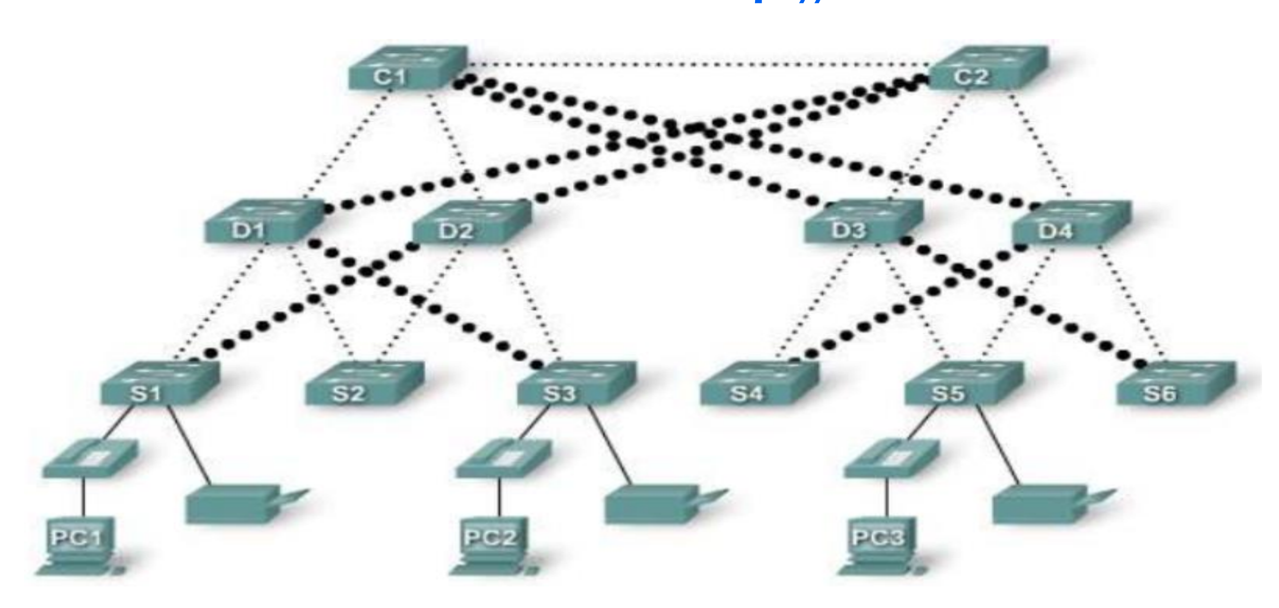


Fig 5 : Liaisons redondantes

2.4. Réseau convergent

Les petites et moyennes entreprises ont dans l'idée d'exécuter des services vocaux et vidéo sur leurs réseaux de données.
La convergence correspond au processus d'association de communications vocale et vidéo sur un réseau de données.

Les réseaux « vocal, vidéo et de données » convergents sont récemment devenus plus populaires sur le marché des petites et moyennes entreprises, en raison de progrès technologiques.
L'un des avantages d'un réseau convergent est qu'il n'y a qu'un réseau à gérer.
La réduction des coûts d'implémentation et de gestion représente un autre avantage. L'implémentation d'une seule infrastructure réseau se révèle moins coûteuse que celle de trois infrastructures réseau distinctes. La gestion d'un réseau unique est également moins onéreuse.

Les réseaux convergents vous fournissent des options qui n'existaient pas précédemment. Vous pouvez dorénavant associer les communications vocale et vidéo directement au sein du système informatique personnel d'un employé. Plus besoin de combiné téléphonique ni de matériel de vidéoconférence coûteux. Vous pouvez obtenir la même fonction à l'aide d'un logiciel spécial intégré à un ordinateur personnel.

Convergence







Fig 6 : Réseau convergent voix, vidéo et données

B. Concepts et configuration de base de la commutation.

I. Fonctionnement d'un commutateur :

1. Fonctions de base d'un commutateur

Une unité de commutation exécute deux fonctions de base :

- La commutation de trames de données : opération qui consiste à recevoir une trame sur une interface du commutateur, de sélectionner l'interface de sortie et de finalement transmettre la trame.
- Gestion des tables de commutation : les commutateurs créent et gèrent des tables de commutation.

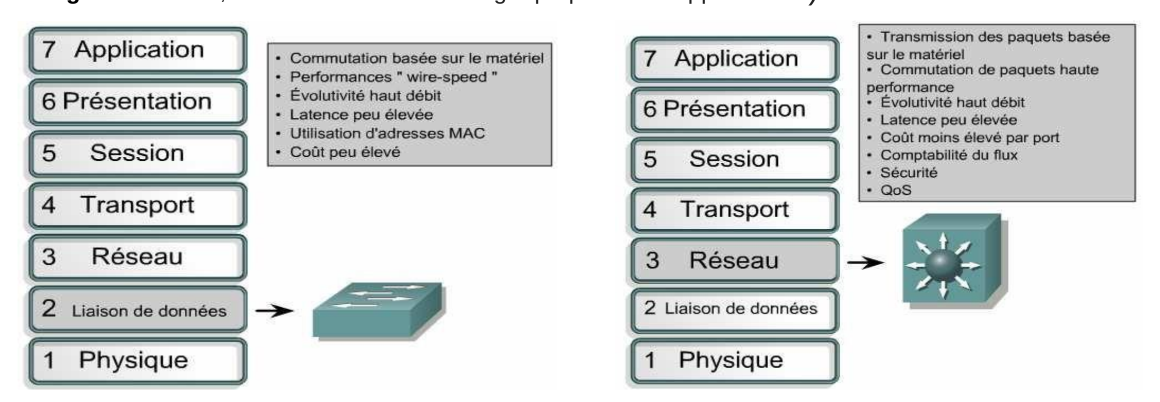
2. Commutation des couches 2 et 3

- Les routeurs et les commutateurs de couche 3 utilisent la commutation de couche 3.
- Les commutateurs de couche 2 et les ponts utilisent la commutation de couche 2.

La différence entre les deux réside au niveau du type d'information utilisé dans la trame pour déterminer l'interface de sortie appropriée (MAC ou IP)

La principale différence entre le processus de commutation de paquet d'un routeur et d'un commutateur de couche 3 se situe au niveau de l'implémentation physique :

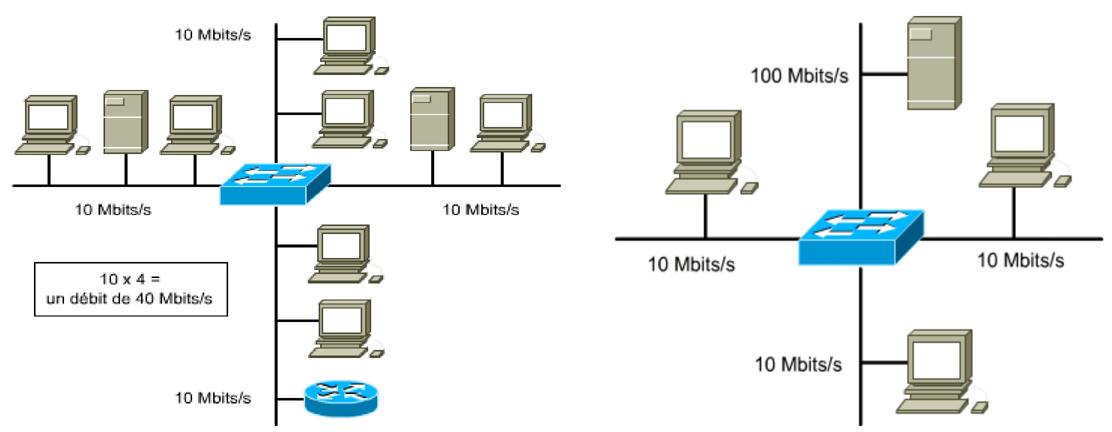
- Dans la plupart des routeurs, la commutation de paquet s'effectue au niveau logiciel par l'intermédiaire d'un microprocesseur.
- Un commutateur de couche 3 effectue la commutation de paquet directement au niveau matériel en ayant recourt à des circuits intégrés spécialisés (ASIC : acronyme de l'anglais **Application-Specific Integrated Circuit**, littéralement « circuit intégré propre à une application »).



3. Commutation symétrique et asymétrique

La commutation symétrique ou asymétrique d'un réseau LAN dépend de la façon dont la bande passante est allouée aux ports de commutateur.

- La commutation symétrique fournit des connexions commutées entre des ports de même débit.
- Un commutateur LAN asymétrique fournit des connexions commutées entre des ports de débits différents, par exemple entre une combinaison de ports de 10 Mbits/s et de 100 Mbits/s.



⟶ Ces techniques de commutation nécessitent l'utilisation d'une mémoire tampon pour conserver les trames contiguës.

4. Mise en mémoire tampon

La zone de mémoire dans laquelle le commutateur stocke les données s'appelle la mémoire tampon.

⟶ Recourir à la mise en mémoire tampon : lorsque le port de destination est occupé ce qui est très souvent dans le cas de la commutation asymétrique.

Cette mémoire peut utiliser deux méthodes pour acheminer les trames :
- la mise en mémoire tampon axée sur les ports
- la mise en mémoire tampon partagée.

• Dans le cas de la mise en mémoire tampon axée sur les ports, les trames sont placées dans des files d'attente liées à des ports entrants spécifiques.
• La mise en mémoire partagée stocke toutes les trames dans une mémoire tampon commune que partagent tous les ports du commutateur.

Le commutateur tient à jour une carte de liaisons entre une trame et un port, indiquant l'emplacement vers lequel un paquet doit être acheminé.

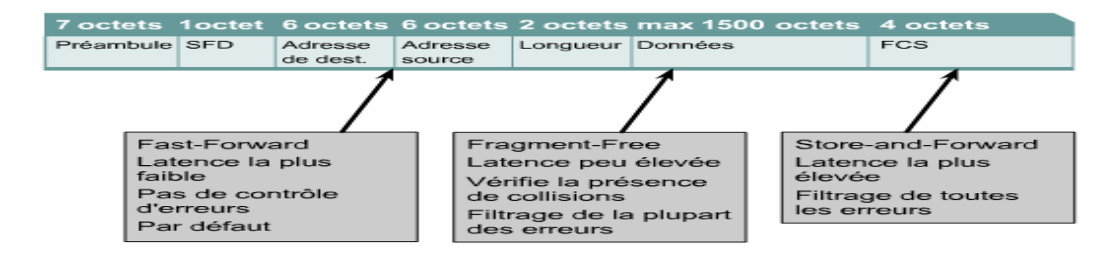
5. Modes de transmission de trame : processus de commutation

Il existe 3 modes de transmission d'une trame :

- Commutation "Cut-through" : la trame est acheminée avant d'avoir été entièrement reçue. Ce mode réduit la latence de la transmission mais diminue aussi le potentiel de détection d'erreurs de commutation. Il y a deux types de commutation "cut-through" :
  - Commutation "Fast-forward" : elle achemine une trame dès la réception de l'adresse MAC de destination. Dans ce mode, la latence est mesurée à partir du premier bit reçu jusqu'au premier bit transmis (c'est la méthode du premier entré, premier sortie ou "FIFO").
  - Commutation "Fragment-free" : elle filtre les fragments de collision avant que l'acheminement ne puisse commencer (fragment < 64 octets), la trame reçue doit être jugée comme n'étant pas un fragment de collision pour être acheminée.

- Commutation "Store-and-Forward" : dans ce mode, la trame doit être reçue entièrement pour qu'elle puisse être acheminée. Le commutateur dispose du temps nécessaire pour vérifier les erreurs, ce qui améliore la détection des erreurs.

- Commutation "Adaptive Cut-through" : elle combine les modes Store-and-Forward et Cut-through. Dans ce mode, le commutateur utilise le mode Cut-through jusqu'à ce qu'il détecte un nombre d'erreurs donné. Une fois le seuil d'erreurs atteint, il passe en mode Store-and-Forward.



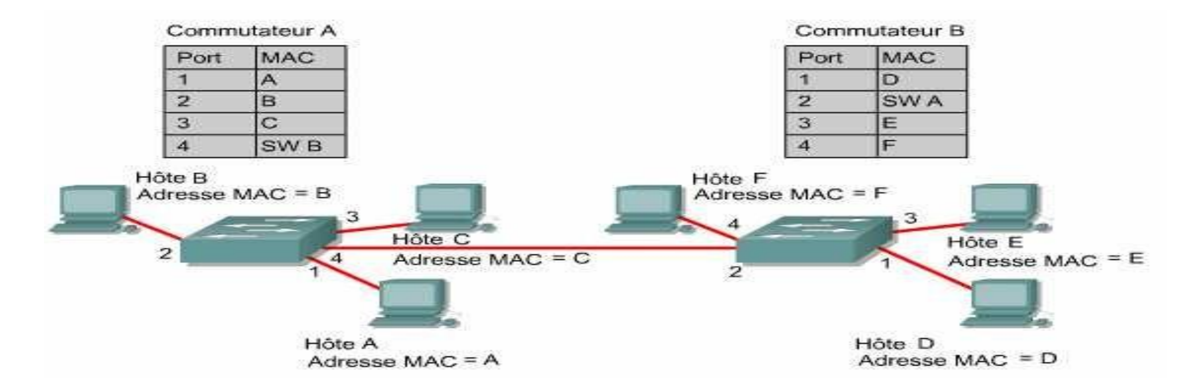
⟶ Latence des commutateurs Ethernet : la latence d'un commutateur est l'intervalle de temps à partir de l'entrée du début d'une trame dans le commutateur jusqu'à la sortie de la fin de la trame correspondante. Cette période est directement liée au processus de commutation configuré et au volume du trafic.

6. Apprentissage des adresses par les commutateurs :

- Lorsqu'un commutateur est activé, des messages de broadcast sont transmis pour demander à toutes les stations du segment local du réseau de répondre.
- Lorsque les stations renvoient le message de broadcast, le commutateur crée une table d'adresses locales. Ce processus est appelé apprentissage.
- Les adresses apprises et l'interface ou le port associé sont stockés dans la table d'adressage.

Remarque : La table d'adressage se trouve dans la mémoire associative (CAM) « Content Addressable Memory ».

Une adresse est horodatée chaque fois qu'elle est enregistrée. Cela permet de stocker les adresses pendant une période déterminée.



Le processus suivi par la mémoire associative (CAM) est le suivant:

- Si l'adresse n'est pas trouvée, le pont achemine la trame sur chaque interface à l'exception de l'interface sur laquelle la trame a été reçue. Ce processus est appelé inondation.
- Si l'adresse est trouvée dans la table d'adresses et que l'adresse est associée à l'interface de réception, la trame est rejetée. Elle doit nécessairement avoir déjà été reçue par la destination.
- Si l'adresse est trouvée dans la table d'adresses et que l'adresse est associée à une interface autre que celle de réception, le pont l'achemine sur l'interface en question.

Lorsque deux hôtes connectés veulent communiquer, le commutateur consulte la table de commutation et établit une connexion virtuelle (micosegment) entre les deux ports. Le circuit virtuel est maintenu jusqu'à ce que la session soit terminée.

II. Configuration de la gestion des commutateurs

1. Démarrage physique du commutateur Catalyst :

Les commutateurs sont des ordinateurs dédiés et spécialisés qui contiennent un CPU, une mémoire RAM et un système d'exploitation.

Un commutateur peut être géré par le biais d'une connexion au port console qui vous permet de consulter et de modifier la configuration.

En règle générale, les commutateurs n'ont pas d'interrupteur d'alimentation permettant de les mettre sous tension ou hors tension. Il y a des modèles avec 24 et 48 ports.



Les deux commutateurs du dessus sont asymétriques et comportent deux ports Gigabit Ethernet fixes pour les médias de cuivre.

2. Indicateurs LED de commutateur

Le panneau avant d'un commutateur comporte différents voyants permettant de surveiller les activités et les performances du système.

Le panneau avant du commutateur comporte les LED suivantes:

- LED système
- LED RPS (Remote Power Supply)
- LEDs pour le mode des ports
- LEDs pour l'état des ports

- La LED système indique si le système est bien alimenté et s'il fonctionne correctement.
- La LED RPS indique si une source de télé-alimentation est utilisée.
- La LED Mode indique l'état actuel du bouton Mode. Les modes permettent de déterminer comment sont interprétés les LED d'état des ports.

Remarque : La signification des LEDs correspondant à l'état des ports varie en fonction de la valeur courante des LEDs Mode.

Led Mode	Couleur	Description
STAT	Désactivé	Aucune liaison
	Vert fixe	Liaison opérationnelle
	Vert clignotant	Le port est en train d'envoyer ou de recevoir des données.
	Alternativement vert/orange	Liaison défectueuse
	Orange fixe	Le port ne transmet pas de données car il a été désactivé par un administrateur ou une violation d'adresse, ou bloqué par le protocole Spanning Tree.
UTIL	Désactivé	Chaque LED éteinte indique une réduction de moitié de la bande passante totale. Les LED sont éteintes de droite à gauche. Si le LED le plus à droite est éteint, le commutateur utilise moins de 50 % de la bande passante totale. Si les deux LED les plus à droite sont éteintes, le commutateur utilise moins de 25 % de la bande passante totale.
	Vert	Si toutes les LED sont vertes, le commutateur utilise au moins 50 % de la bande passante totale.
DUPLX	Désactivé	Le port fonctionne en mode half-duplex.
	Vert	Le port fonctionne en mode full duplex.
SPEED	Désactivé	Le port fonctionne à 10 Mbits/s.
	Vert	Le port fonctionne à 100 Mbits/s.
	Vert clignotant	Le port opère à 1000 Mbits/s

Vérification des LEDs au cours du test (POST)

LED système
La LED système indique le succès ou l'échec de POST. • Si la LED système est éteinte alors que le commutateur est connecté, le test POST est en cours. • Si la LED système est verte, le test POST a réussi. • Si la LED système est orange, le test POST a échoué.

Les LED d'état des ports peuvent également changer de couleur pendant le test POST du commutateur.

Elles peuvent devenir orange pendant 30 secondes, juste le temps pour le commutateur de découvrir la topologie du réseau et de rechercher d'éventuelles boucles.

- LED verte : le commutateur a établi un lien entre le port et une cible
- LED s'éteigne : le commutateur a déterminé que rien n'est connecté au port

3. Affichage des informations après démarrage initial du commutateur

- Connectez un ordinateur à ce commutateur « un câble à paires inversées »
- Lancez HyperTerminal sur l'ordinateur et définir les paramètres par défaut.
- Branchez le commutateur à une prise murale.

Les informations délivrées après le démarrage initial du commutateur devraient s'afficher sur l'écran HyperTerminal. Cet affichage présente des informations sur le commutateur, des détails sur l'état du POST et des données sur le matériel du commutateur.

Aperçu de l'aide de l'interface de commande en ligne du commutateur

? ⟶ Affiche la liste des commandes disponibles pour le mode de commande actuel.

? ⟶ Aide sur les termes pour accomplir la suite d'une commande.

? ⟶Aide à la syntaxe des commandes et fournit des mots clés en fonction d'une commande.

Modes de commande des commutateurs

Le mode par défaut est le mode utilisateur (User EXEC mode) « > ».

Les commandes disponibles en mode utilisateur sont celles qui permettent de modifier les paramètres du terminal, de réaliser des tests de base et d'afficher les informations système.

Commandes	Description
show version	Affiche les informations de version du logiciel et du matériel. Utilisé afin de déterminer exactement le logiciel et les modules en cours d'utilisation.
show flash:	Affiche l'information à propros du système de fichiers flash: .
show mac-address-table	Affiche les adresses MAC contenues dans la table de con
show controllers ethernet-controller	Indique les trames abandonnées ou différées, les erreurs d'alignement, les collisions, etc.

La commande enable est utilisée pour passer au mode privilégié. « # ».

Commandes	Description
show running-config	Affiche le fichier de configuration courant du commutateur.
show post	Indique si commutateur a réussi son test automatique de mise sous tension (POST)
show vlan	Vérifie la configuration VLAN.
show interfaces	Affiche la configuration et l'état d'une interface.

4. Configuration des commutateurs :

a. Vérification de la configuration par défaut du commutateur Catalyst

Par défaut : Le nom d'hôte est Switch + Aucun mot de passe n'est défini sur les lignes de console ou de terminal virtuel + pas d'adresse IP configurée + Les ports ou interfaces du commutateur sont définis sur le mode automatique + tous les ports du commutateur se trouvent dans le VLAN 1 + Le répertoire flash comporte un fichier qui contient l'image IOS, un fichier nommé env_vars et un sous-répertoire nommé html + Le protocole STP est activé

- Il est possible de donner une adresse IP à un commutateur pour des raisons d'administration. Il faut configurer cette adresse au niveau de l'interface virtuelle, VLAN 1.

- Une fois que le commutateur est configuré, le répertoire flash peut également contenir un fichier config.text et une base de données VLAN.

Show running-config ⟶vérifier la configuration actuelle

Show version ⟶ vérifier les paramètres de version IOS et du registre de configuration.

b. Pour réinitialiser la configuration d'un commutateur :

Catalyst 2950

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<Affichage tronqué>
Switch#reload
```

→ Supprimez toutes les informations VLAN existantes.

→ Supprimez le fichier de configuration sauvegardé startup-config.

→ Rechargez le commutateur

Catalyst 1900

```
Switch#delete nvram
```

c. Définir un nom au commutateur + Mots de passe → mêmes commandes qu'un routeur.

d. Définition des paramètres de vitesse de port et de mode duplex :

Duplex full → pour activer le mode full duplex (à partir du mode d'interface)

Speed {débit} → pour définir la vitesse de l'interface (à partir du mode d'interface).

e. Configuration à partir d'un navigateur :

Les commutateurs peuvent offrir une interface Web à des fins de configuration et de gestion. Un navigateur Web peut accéder à ce service en utilisant l'adresse IP et le port 80.

Ip http server → pour activer le service Http

Ip http port 80 → pour définir le port utilisé.

f. Gestion du fichier de système d'exploitation du commutateur

Un administrateur devrait documenter et gérer les fichiers de configuration opérationnels des équipements réseau.

- Le fichier de la configuration courante le plus récent devrait être sauvegardé sur un serveur ou un disque.
- L'IOS devrait également être sauvegardée sur un serveur local.
- S'avérer extrêmement utile le jour où une configuration doit être restaurée.

Procédures de Gestion de fichier de l'IOS :

- Copie de l'IOS sur un serveur TFTP :

Copy flash:c2900XL-hs-mz-112.8.10-SA6.bin tftp
+ Confirmer + indiquer l'adresse IP + Entrée

- Copie de l'IOS à partir du serveur TFTP :

Copy tftp flash
+ Indiquer l'@IP du serveur + indiquer le nom du fichier + confirmer
Remarque : Lors du téléchargement du fichier : l'écran affiche des !!!!!!!!!!!!!!

Procédures de Gestion de fichier de configuration :

- Copie du fichier sur un serveur TFTP :

Copy start tftp
+ indiquer l'@IP + nom de fichier

Remarque : Pour les Catalyst 1900 : copy nvram tftp://192.168.1.3/alswitch-config

- Copie de l'IOS à partir du serveur TFTP :

1- vous devez d'abord effacer le commutateur
2- Reconfigurez le commutateur avec une adresse IP VLAN 1.
3- tapez la commande ***copy tftp startup-config***
+ indiquer l'@IP du serveur + le nom de fichier.

g. Gestion de la table d'adresses MAC

Show mac-address-table ⟶ Pour afficher les adresses apprises par un commutateur.

Si aucune trame n'est interceptée avec l'adresse apprise précédemment, l'entrée correspondante est automatiquement supprimée dans la table d'adresses MAC ou expire au bout de 300 secondes.

Pour ne pas surcharger la mémoire et optimiser le fonctionnement du commutateur, les adresses apprises peuvent être supprimées de la table d'adresses MAC.

Clear mac-address-table dynamic ⟶ Pour supprimer les entrées apprises dynamiquement

h. Configuration d'adresses MAC statiques

Switch(config)#mac-address-table static <adresse-mac de l'hôte> interface FastEthernet <numéro Ethernet> vlan <nom vlan> ⟶ Pour affecter une adresse MAC de façon permanente à une interface

Voici certaines de ces raisons pour définir une @MAC :

- L'adresse MAC ne doit jamais être supprimée automatiquement par le commutateur.
- Un serveur spécifique doit être attaché au port et l'adresse MAC est connue.
- Améliorer la sécurité.

i. Configuration de la sécurité des ports

Le nombre d'adresses MAC par port peut être limité à 1. La première adresse apprise par le commutateur de façon dynamique devient l'adresse sécurisée.

Switchport port-security {@MAC} ⟶ Configurer la sécurité d'un port (mode d'interface)

Show port security ⟶ pour vérifier l'état de sécurité du port.

j. Exécution d'ajouts, de déplacements et de modifications

Lorsqu'un nouveau commutateur est ajouté à un réseau, configurez les éléments suivants :

- Le nom du commutateur
- L'adresse IP du commutateur dans le VLAN d'administration
- Une passerelle par défaut
- Les mots de passe de ligne

Lorsqu'un hôte passe d'un port ou d'un commutateur à un autre, il est préférable de supprimer les configurations pouvant entraîner un comportement inattendu. La configuration requise peut ensuite être ajoutée.

k. Procédure de récupération de mots de passe 1900/2950

- Mettre le commutateur sous tension en maintenant enfoncé le bouton « MODE ». Relâchez le bouton dès la LED STAT
- Pour initialiser le système de fichiers et terminer le chargement :

flash_init
load_helper
dir flash

Rename flash:config.text flash:config.old ⟶ Renommer le fichier de config

Reload ⟶ Redémarrer le système

Boot ⟶ Répondre « No » pour annuler le dialogue de configuration.

Rename flash:config.old flash:config.text ⟶ Renommer à nouveau le fichier de config

Copy flash: config.text system: running-config ⟶ Copier le fichier de conf en mémoire

⟶ Modifier les anciens mots de passé.

⟶ Sauvegarder la configuration.

⟶ Mettez le commutateur hors tension puis sous tension et vérifiez les MDP

I. Mise à jour du firmware 1900/2950

Show boot ⟶Pour afficher le nom de fichier d'image active

Si aucune image logicielle n'est définie dans le chemin d'amorçage, entrez ***dir flash*** ou ***Show flash***

```
ALSwitch#dir flash:
Directory of flash:/

2 -rwx 1674921 Mar 01 1993 01:28:10 c2950-c3h2s-mz.120-5.3.WC.1.bin
3 -rwx 269 Jan 01 1970 00:00:57 env_vars
4 drwx 10240 Mar 01 1993 00:21:13 html
165-rwx 965 Mar 01 1993 00:22:23 config.text

7741440 bytes total (4778496 bytes free)
```

⟶ Renommer le fichier IOS existant avec le même nom et avec l'extension .old

```
ALSwitch#rename flash:c2950-c3h2s-mz.120-5.3.WC.1.bin flash:c2950-
c3h2s-mz.120-5.3.WC.1.old
```

Dir flash ⟶ pour vérifier le nouveau nom

Switch(config)#no ip http server ⟶Désactiver l'accès aux pages HTML du commutateur:

Switch#delete flash:html/* ⟶Supprimer les fichiers HTML existants.

⟶ Extraire la nouvelle image de l'IOS et les nouveaux fichiers HTML de la mémoire flash:
Switch#archive tar /x tftp://192.168.1.3/c2950-c3h2s-mz.120- 5.3.WC.1.tar flash:

Switch(config)#ip http server ⟶ Réactivez l'accès aux pages HTML du commutateur:

⟶ Associez le nouveau fichier d'amorçage

Switch (config)#boot system flash:c2950-c3h2s-mz.120-5.4.WC.1.bin

⟶ Redémarrer le commutateur et vérifier et supprimer l'ancienne image :

Reload ⟶ pour redémarrer

Show version ⟶ Pour vérifier l'image de démarrage.

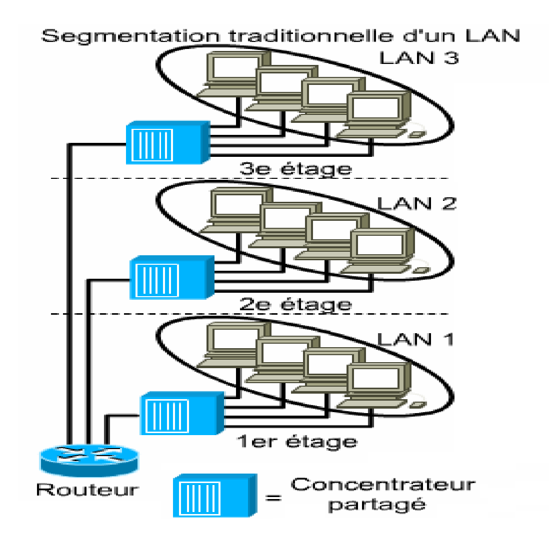
Delete flash:c2950-c3h2s-mz.120-5.3.WC.1.old ⟶ Supprimer l'image ancienne.

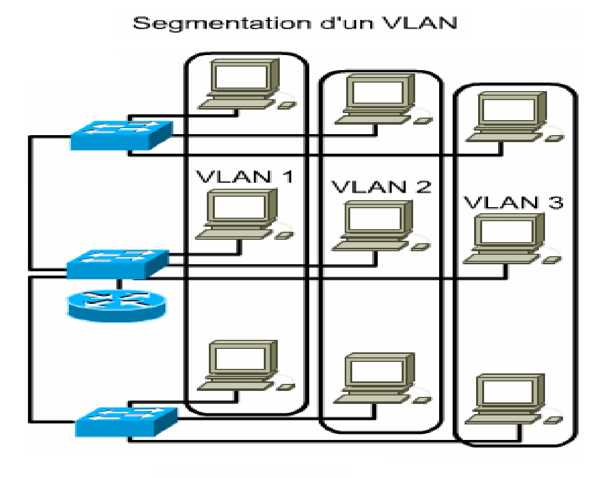
C. Les réseaux locaux virtuels.

I. Introduction au LAN Virtuel :

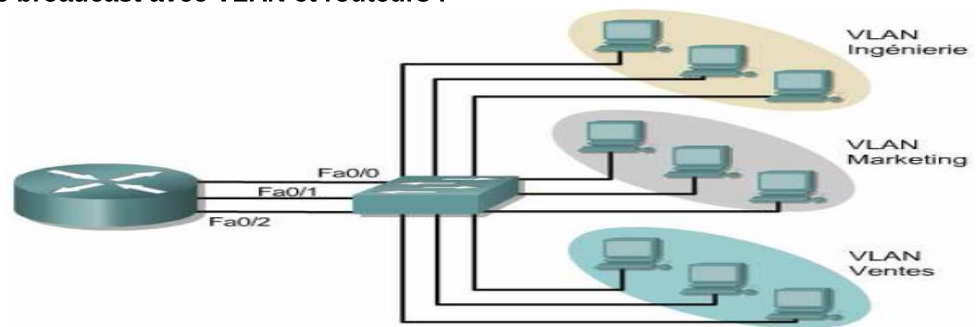
- Un LAN virtuel (ou **VLAN**) est un groupe de services réseau qui ne sont pas limités à un segment physique ou à un commutateur LAN.
- Les VLAN segmentent les réseaux commutés de manière logique sur la base des fonctions, des équipes de projet ou des applications de l'entreprise, quel que soit l'emplacement physique ou les connexions au réseau.
- Les LAN virtuels segmentent logiquement le réseau en différents domaines de broadcast. Les commutateurs LAN utilisent des protocoles de pontage avec un groupe de ponts distinct pour chaque VLAN.
- Les VLAN sont créés pour fournir des services de segmentation habituellement fournis par les routeurs physiques dans les configurations LAN. Les VLAN répondent aux problèmes d'évolutivité, de sécurité et de gestion des réseaux.

Remarque : Les commutateurs ne peuvent pas acheminer de paquets entre des VLAN par le biais de ponts.





Domaines de broadcast avec VLAN et routeurs :



Dans cet exemple, 3 VLAN sont créés avec un routeur et un commutateur. Toutefois, il y a trois domaines de broadcast séparés. Dans ce scénario, il y a *un routeur* et un commutateur, mais *trois domaines de broadcast* séparés.
Le commutateur transmet les trames des VLAN Ingénierie, Marketing et Ventes respectivement aux sous interfaces du routeur Fa0/0, Fa0/1 et Fa0/2:

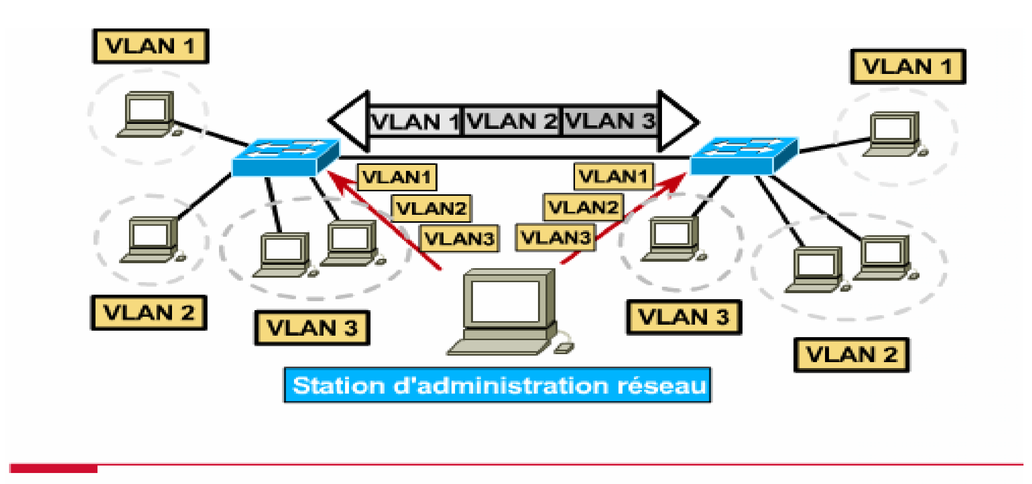
Avantages des VLAN :
Le principal avantage des VLAN est qu'ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes:

- Déplacer facilement des stations de travail sur le LAN
- Ajouter facilement des stations de travail au LAN
- Modifier facilement la configuration LAN
- Contrôler facilement le trafic réseau
- Améliorer la sécurité

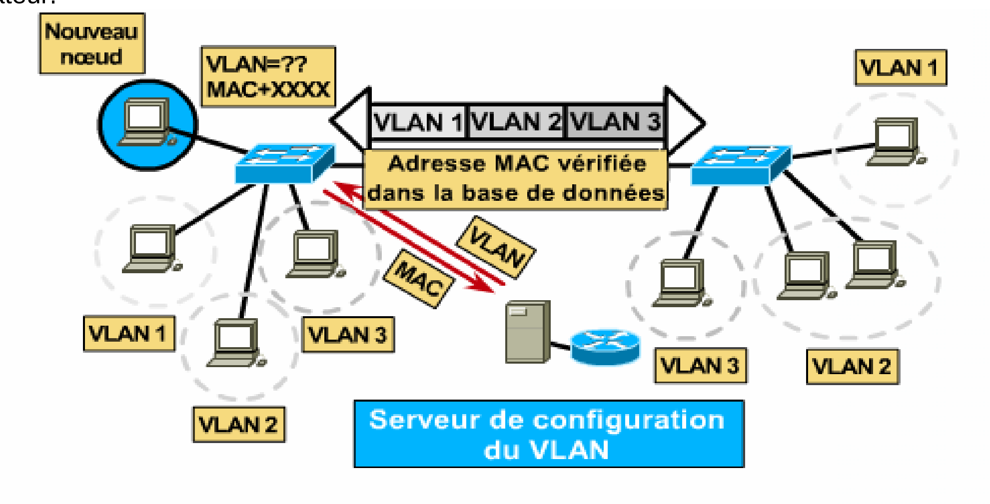
II. Fonctionnement d'un VLAN :

Chaque port de commutateur peut être attribué à un LAN virtuel différent. Les ports affectés au même LAN virtuel partagent les broadcasts.

- Les **VLAN statiques** sont dits «*axés sur le port*». Lorsqu'un équipement accède au réseau, il adopte automatiquement le VLAN d'appartenance du port auquel il est connecté.
  Les LAN virtuels offrent aux utilisateurs une bande passante plus large qu'un réseau partagé. *Le VLAN par défaut* de chaque port du commutateur est le ***VLAN de gestion***. Par défaut, le VLAN 1 est toujours le VLAN de gestion et ne peut pas être supprimé. Au moins un des ports doit être dans ce VLAN.



- Les **VLAN dynamiques** sont créés par l'intermédiaire du logiciel d'administration réseau. CiscoWorks 2000 ou CiscoWorks for Switched Internetworks est utilisé pour créer des VLAN dynamiques. Les VLAN dynamiques permettent une appartenance axée sur l'adresse MAC de l'unité connectée au port du commutateur.



III. Différents types des LAN virtuels (VLAN) :

Une adresse réseau de couche 3 unique doit être affectée à chaque VLAN. Cela permet aux routeurs de commuter les paquets entre les VLAN.
Les VLAN peuvent être créés sous forme de réseaux de bout en bout ou exister à l'intérieur de frontières géographiques.

- **Les VLAN de bout en bout** permettent de regrouper les équipements en fonction de l'utilisation des ressources. Cela inclut des paramètres comme l'utilisation du serveur, les équipes de projet et les services. Le but des VLAN de bout-en bout est de maintenir 80 % du trafic sur le VLAN local.
  Un réseau VLAN de bout en bout a les caractéristiques suivantes :
  - Les utilisateurs sont regroupés en VLAN qui dépendent de leur groupe de travail ou de leur fonction, mais pas de leur localisation physique.
  - Lorsqu'un utilisateur se déplace sur le campus, son appartenance à un VLAN ne doit pas changer.
  - Chaque VLAN est caractérisé par un ensemble commun de besoins de sécurité pour tous les membres.

  À partir de la couche accès, des ports de commutation sont fournis pour chaque utilisateur. En raison du déplacement des personnes, chaque commutateur devient finalement un membre de tous les VLAN.
  Il a été tenté de garder les utilisateurs dans le même VLAN que leur serveur afin d'optimiser les performances de commutation de couche 2 et de centraliser le trafic.
  Un routeur de couche principale est utilisé pour acheminer les paquets entre les sous réseaux.
  Le réseau est conçu sur la base de modèles de flux de trafic de telle sorte que 80 % du trafic soit contenu au sein d'un VLAN. Les 20 % restants traversent le routeur jusqu'aux serveurs d'entreprise et jusqu'aux réseaux Internet et WAN.

- **VLAN géographiques :** dans cette structure, la nouvelle règle 20/80 est très fréquemment appliquée. 80 % du trafic est effectué à distance pour l'utilisateur contre 20 % en local. Bien que cette topologie implique pour l'utilisateur de traverser une unité de couche 3 afin d'atteindre 80 % des ressources, cette configuration permet au réseau de fournir une méthode cohérente et déterministe d'accès aux ressources.

IV. Etiquetage des trames

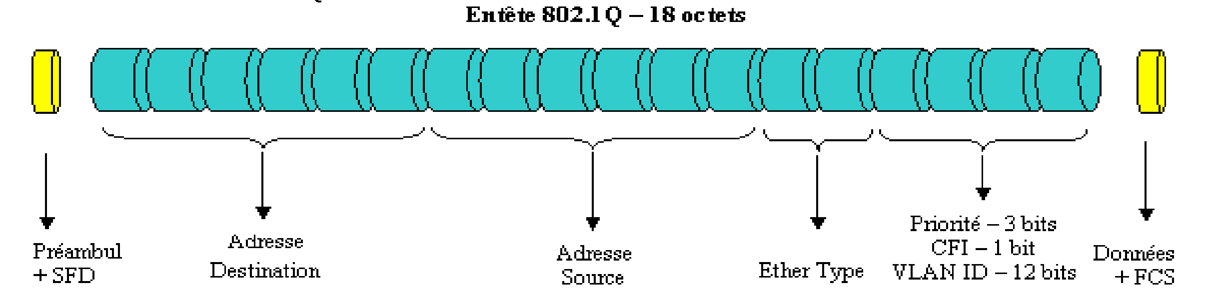
Lorsque des trames sont reçus par le commutateur à partir d'une station, un identifiant de trame unique est ajouté dans chaque en-tête. Cette information d'en-tête désigne l'appartenance à un VLAN de chaque trame. La trame est ensuite transmise aux commutateurs ou routeurs appropriés sur la base de l'ID de VLAN et de l'adresse MAC. Sur le nœud de destination, l'ID du VLAN est supprimé de la trame par le commutateur contigu et transmis à l'unité connectée.

Étiquetage	Méthode	Médias	Description
ISL (Inter-Switch Link)	Fast Ethernet	L'en-tête ISL encapsule la trame LAN et contient un champ ID de VLAN.	La trame est allongée.
802.1Q	Fast Ethernet	Protocole VLAN Ethernet défini par l'IEEE.	L'en-tête est modifié.
Émulation de LAN (LANE)	ATM	Aucune étiquetage	Une connexion virtuelle implique un ID de VLAN.

Remarque : Les commutateurs Catalyst 2950 ne prennent pas en charge l'agrégation ISL.

Normalisation IEEE 802.1q.

Le protocole 802.1Q permet de réaliser des réseaux locaux virtuels sur une architecture Ethernet. Ces réseaux privés sont appelés VLAN. Pour cela, 4 octets sont ajoutés à l'entête Ethernet classique permettant, principalement, d'indiquer le numéro de VLAN et donc l'ID du sous réseau.
Voici l'entête d'une trame 802.Q :



CFI : (Canonial Format Indicator)

V. Configuration des VLAN statiques :

Les lignes directrices suivantes doivent être suivies lors de la configuration de VLAN sur des commutateurs Cisco 29xx:

- Le nombre maximum de VLAN dépend du commutateur.
- Le VLAN 1 est le VLAN Ethernet par défaut.
- Des annonces CDP et VTP sont envoyées sur le VLAN 1.
- L'adresse IP de Catalyst est associée par défaut au domaine de broadcast du VLAN 1.
- Le commutateur doit être en mode serveur VTP pour créer, ajouter ou supprimer des VLAN.

Créer un VLAN :

Switch#Vlan database
Switch(vlan)#Vlan **{ID_vlan}**
Switch(vlan)#Exit

Affecter une interface à un VLAN :

Switch(config-if)#Switchport mode access vlan
Switch(config-if)#Switchport access vlan **{ID_vlan}**

Vérification de la configuration VLAN

Show vlan
Show vlan brief
Show vlan id **{ID_vlan}**

```
SydneySwitch#show vlan

VLAN Name                 Status    Ports
---- -------------------- -------- -------------------------------

VLAN Name                 Status    Ports
---- -------------------- -------- ----------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/4
2    VLAN2                active    Fa0/3, Fa0/5, Fa0/6, Fa0/7
3    VLAN3                active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                    Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

Enregistrement de la configuration VLAN

Il est souvent utile de garder une copie de la configuration VLAN sous forme de fichier texte à des fins de sauvegarde ou d'audit.

Suppression de VLAN

Pour enlever une interface d'un VLAN :

Switch(config-if)#No switchport access vlan **{ID_vlan}**

Pour enlever un VLAN entièrement d'un commutateur, entrez les commandes:

Switch(vlan)#No vlan {ID}

Remarque : Lorsqu'un VLAN est supprimé, tous les ports qui lui sont affectés deviennent inactifs. Toutefois, ces ports restent associés au VLAN supprimé jusqu'à ce qu'ils soient affectés à un nouveau VLAN.

Dépannage des VLAN

- Vérifiez qu'une adresse IP est configurée sur l'interface Fast Ethernet.
- Des adresses IP sont configurées sur chaque sous-interface d'une connexion VLAN.
- Vérifiez que la configuration duplex sur le routeur correspond à celle du port ou de l'interface approprié(e) sur le commutateur.

D. Protocole VTP.

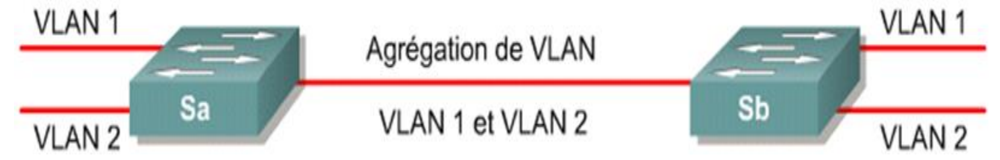
I. Agrégation (Trunking)

1. Concepts d’agrégation

La figure suivante illustre deux VLAN répartis sur deux commutateurs (Sa et Sb). Chaque commutateur utilise deux liaisons physiques, de sorte que chaque port transporte le trafic d’un VLAN unique. Il s’agit de la méthode la plus simple de mise en œuvre d’une communication VLAN entre commutateurs, mais elle n’offre pas une évolutivité suffisante.



Dans le contexte d’un environnement de commutation VLAN, une agrégation de VLAN est une liaison point-à-point physique ou logique qui prend en charge plusieurs VLAN. L’objectif d’une agrégation de VLAN est d'économiser des ports lors de la création d’une liaison entre deux unités contenant des VLAN.



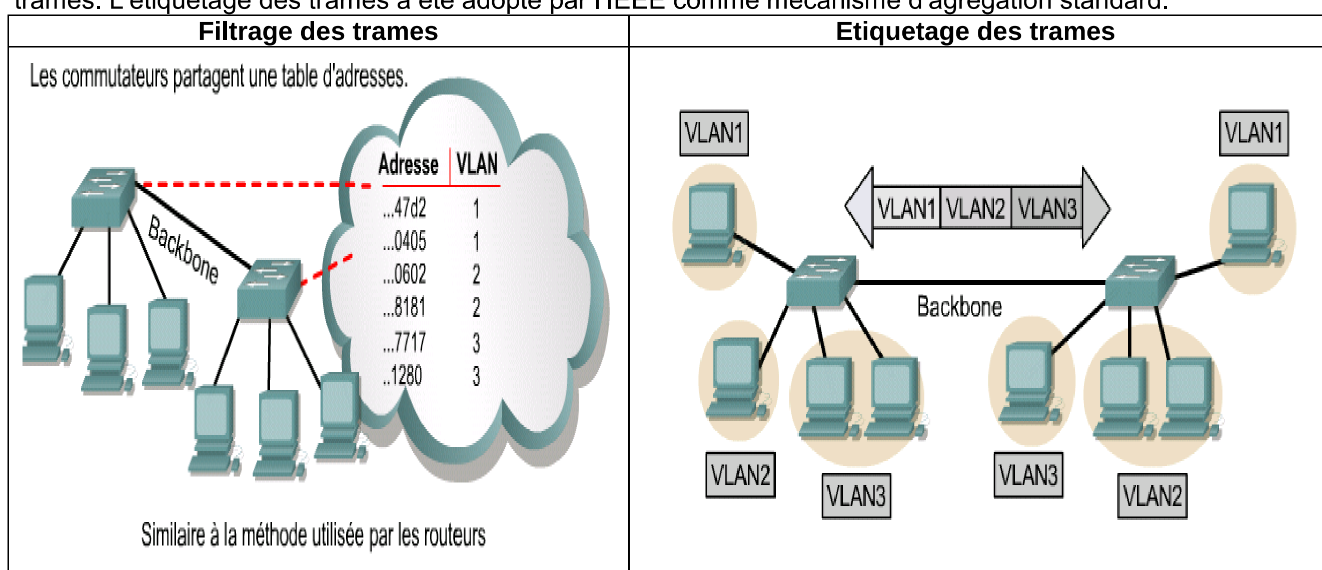
2. Fonctionnement d’une agrégation de VLAN

Les tables de commutation aux deux extrémités de l’agrégation peuvent être utilisées pour prendre des décisions de transmission sur la base des adresses MAC de destination des trames. Lorsque le nombre de VLAN circulant sur l’agrégation augmente, les décisions de transmission deviennent plus difficiles à gérer. Le processus de prise de décision est ralenti car le traitement de tables de commutation volumineuses prend plus de temps.

Des protocoles d’agrégation ont été développés pour gérer efficacement le transfert de trames de différents VLAN sur une liaison physique unique. Les protocoles d’agrégation définissent un consensus pour la distribution de trames aux ports associés aux deux extrémités de l’agrégation.

Actuellement, il existe deux types de mécanismes d’agrégation: le filtrage des trames et l’étiquetage des trames. L’étiquetage des trames a été adopté par l’IEEE comme mécanisme d’agrégation standard.

Filtrage des trames	**Etiquetage des trames**



La liaison physique unique entre les deux commutateurs est capable de transporter le trafic pour n’importe quel VLAN. Pour cela, chaque trame envoyée sur la liaison est étiquetée afin d’identifier le VLAN auquel elle appartient. Il existe plusieurs systèmes d’étiquetage. Les systèmes d’étiquetage les plus courants pour les segments Ethernet sont répertoriés ci-dessous:

- **ISL** (Inter-Switch Link) – Protocole propriétaire de Cisco
- **802.1Q** – Norme IEEE plus particulièrement traitée dans cette section

II. VTP (Virtual Trunking Protocol)

1. Concepts de VTP

Les commutateurs VTP exécutent l'un des trois modes suivants:

- Serveur
- Client
- Transparent

Les serveurs VTP peuvent créer, modifier et supprimer un VLAN et des paramètres de configuration VLAN pour l'ensemble du domaine. Les serveurs VTP enregistrent les informations de configuration VLAN dans la mémoire NVRAM du commutateur. Les serveurs VTP envoient des messages VTP par tous les ports multi-VLAN.
Les clients VTP ne peuvent pas créer, modifier ou supprimer des informations VLAN. Ce mode est utile pour les commutateurs qui manquent de mémoire pour stocker de grandes tables d'informations VLAN. Le seul rôle des clients VTP est de traiter les modifications VLAN et d'envoyer des messages VTP par tous les ports multi-VLAN.
Les commutateurs en mode transparent VTP transmettent des annonces VTP mais ignorent les informations contenues dans le message. Un commutateur transparent ne modifie pas sa base de données lors de la réception de mises à jour et il n'envoie pas de mises à jour indiquant une modification apportée à son état VLAN. Excepté pour la transmission d'annonces VTP, le protocole VTP est désactivé sur un commutateur transparent.

2. Configuration de VTP

Les tâches de base suivantes doivent être effectuées avant de configurer le protocole VTP et les VLAN sur le réseau.

1. Déterminez le numéro de la version de VTP qui sera utilisée.
2. Indiquez si ce commutateur sera un membre d'un domaine de gestion existant ou si un nouveau domaine doit être créé.
3. Choisissez un mode VTP pour le commutateur.

Deux versions différentes de VTP sont disponibles: la version 1 et la version 2. La version 2 de VTP peut être mise en œuvre pour la prise en charge des VLAN Token Ring.

Pour configurer la version de VTP sur un commutateur à base de commandes Cisco IOS, passez d'abord en mode base de données VLAN.

Utilisez la commande suivante pour changer le numéro de version de VTP:

Switch#**vlan database**
Switch(vlan)#**vtp v2-mode**

Pour créer un domaine de gestion, utilisez la commande suivante:

Switch(vlan)#**vtp domain cisco**

Le nom du domaine peut comporter entre 1 et 32 caractères. Le mot de passe peut comporter entre 8 et 64 caractères.

Pour définir le mode approprié du commutateur à base de commandes Cisco IOS, utilisez la commande suivante:

Switch(vlan)#**vtp {client | server | transparent}**

La figure suivante présente les informations affichées par la commande **show vtp status**. Cette commande permet de vérifier les paramètres de configuration VTP sur un commutateur à base de commandes Cisco IOS.

```
MDF_Switch#show vtp status
VTP Version                          :2
Configuration Revision               :0
Maximum VLANs supported locally      :64
Number of existing VLANs             :7
VTP Operation Mode                   :Server
VTP Domain Name                      :cisco
VTP Pruning Mode                     :Disabled
VTP V2 Mode                          :Disabled
VTP Traps Generation                 :Disabled
MD5 digest                           :0x30 0x50
Configuration last modified by 10.1.1.252 a local
updater ID 138.25.13.121 on interface found)
MDF_Switch#exit
```

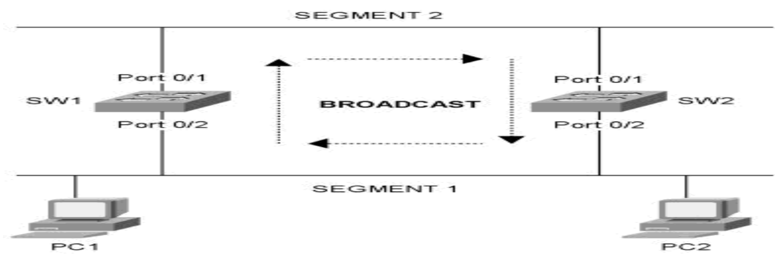
E. Protocole STP.

Le protocole Spanning Tree (STP) est un protocole de couche 2 (liaison de données) conçu pour les switchs et les bridges. La spécification de STP est définie dans le document IEEE 802.1d. Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité.

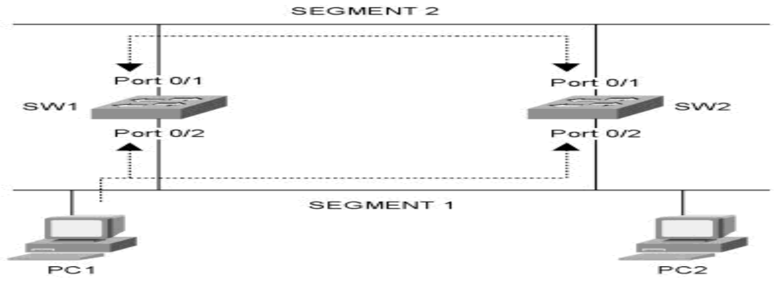
I. PROBLÉMATIQUE

Dans un contexte de liaisons redondantes sans STP deux problèmes peuvent survenir :

1.1. Des tempêtes de broadcast : lorsque des trames de broadcast sont envoyées (FF-FF-FF-FF-FF-FF en destination), les Switchs les renvoient par tous les ports. Les trames circulent en boucles et sont multipliées. Les trames n'ayant pas de durée de vie (TTL comme les paquets IP), elles peuvent tourner indéfiniment.



1.2. Une instabilité des tables MAC : quand une trame, même unicast, parvient aux Switchs connectés en redondance, le port du Switch associé à l'origine risque d'être erroné. Une boucle est susceptible d'être créée.



Dans cet exemple, le PC1 envoie une trame au PC2. Les deux commutateurs reçoivent la trame sur leur port 0/2 et associent ce port à l'adresse mac de PC1. Si l'adresse de PC2 est inconnue, les deux commutateurs transfèrent la trame à travers leur port 0/1. Les commutateurs reçoivent respectivement ces trames inversement et associent l'adresse MAC de PC1 au port 0/1. Ce processus peut se répéter indéfiniment.

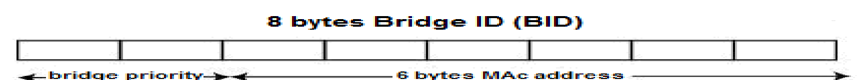
II. FONCTIONNEMENT DE STP

Bien que cette topologie physique puisse fournir de multiples chemins dans un contexte de redondance et ainsi améliorer la fiabilité d'un réseau, STP crée un chemin sans boucle basé sur le chemin le plus court. Ce chemin est établi en fonction de la somme des coûts des liens entre les Switchs, ce coût étant basé sur la vitesse d'un port. Aussi, un chemin sans boucle suppose que certains ports soient bloqués et pas d'autres. STP échange régulièrement des informations (**appelées des BPDU - Bridge Protocol Data Unit**) afin qu'une éventuelle modification de topologie puisse être adaptée sans boucle.

2.1. Sélection d'un switch Root

Le Switch Root sera le point central de l'arbre STP. Le Switch qui aura l'ID la plus faible sera celui qui sera élu Root. L'ID du Switch comporte deux parties, d'une part, la priorité (2 octets) et, d'autre part, l'adresse MAC (6 octets). La priorité 802.1d est d'une valeur de 32768 par défaut (ce sont des multiples de 4096 sur 16 bits). Par exemple, un Switch avec une priorité par défaut de32768 (8000 Hex) et une adresse MAC 00 :A0 :C5:12:34:56, prendra l'ID 8000:00A0:C512:3456. On peut changer la priorité d'un Switch avec la commande :

(config)#**spanning-tree [vlan** *vlan-id*] **priority** *priority*



Sur un Switch Root, **tous les ports sont des ports désignés**, autrement dit, ils sont en état « forwarding », ils envoient et reçoivent le trafic.

2.2. Sélection d'un port Root pour les Switch non-root.

Chaque Switch non-root va sélectionner un port Root qui aura le chemin le plus court vers le Switch Root. Normalement, un port Root est en état « forwarding ».

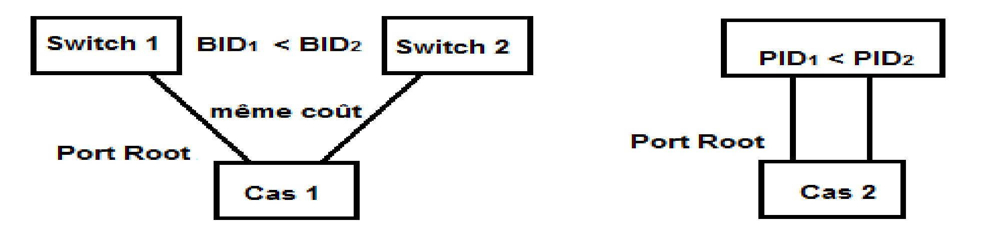
Vitesse du lien	Coût	Plage de coût recommandée
4Mbps	250	100 to 1000
10Mbps	100	50 to 600
16Mbps	62	40 to 400
100Mbps	19	10 to 60
1Gbps	4	3 to 10
10Gbps	2	1 to 5

Le coût d'une liaison peut être configuré sur le port considéré en utilisant la commande suivante :

(config-if)#**spanning-tree cost** *cost* (s'il s'agit d'un port d'accès)
(config-if)#**spanning-tree vlan** *vlan-id* **cost** *cost* (s'il s'agit d'un port de tronc)

A noter aussi qu'en cas de coûts égaux le port Root est :

- celui qui est relié au Switch de BID le plus faible (cas 1).
- celui qui est relié au port de PID le plus faible (cas 2).



PID étant l'ID du port composé de 2 octets (priorité + numéro du port).
La priorité d'un port est égale à 128 par défaut et peut être configurée de 0 à 255 en utilisant la commande suivante :

(config-if)#**spanning-tree port-priority** *priority* (s'il s'agit d'un port d'accès)
(config-if)#**spanning-tree vlan** *vlan-id* **port-priority** *priority* (s'il s'agit d'un port de tronc)

2.3. Sélection d'un port désigné pour chaque segment

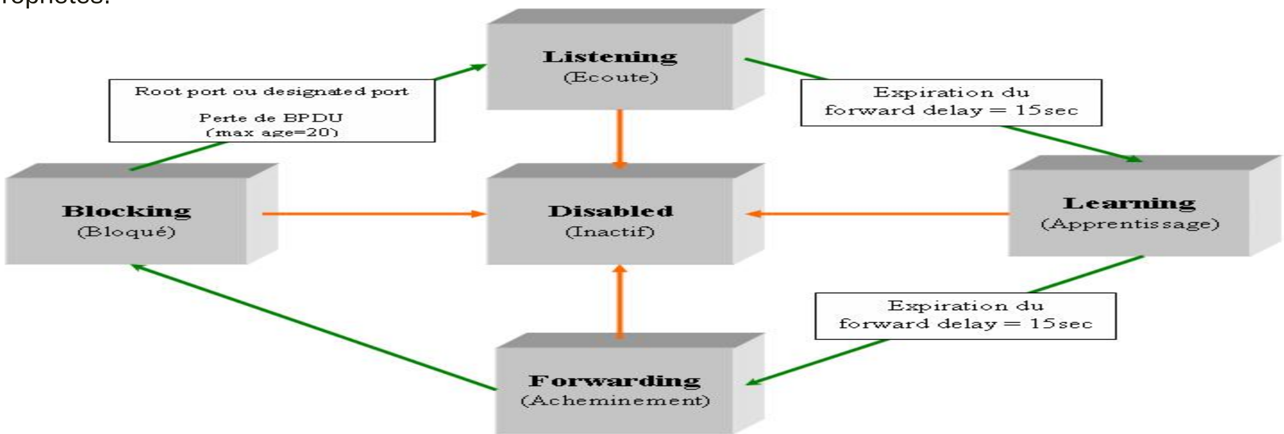
Pour chaque segment d'un Lan (domaine de collision), il y a un port désigné. Le port désigné est celui qui a le chemin le plus court vers le bridge Root. Les ports désignés sont normalement en état « forwarding », autrement dit, envoient et reçoivent du trafic de données. Si plus d'un port sur un même segment a le même coût vers le Switch Root, le port du Switch qui a l'ID la plus faible est choisi. Tous les autres sont des ports non-désignés en état « blocking ».

En bref,

> **1 Switch Root par réseau dont tous les ports sont désignés**
> **1 port Root par Switch non-root**
> **1 port désigné par domaine de collision**
> **tous les autres ports sont non-désignés**

III. DIFFÉRENTS ÉTATS STP

Cinq états de ports peuvent être rencontrés sur un port STP. Chaque état comporte un délai. En voici les propriétés.



L'âge maximal de 20 secondes par défaut est le temps maximal avant que STP effectue de nouveaux calculs quand une interface ne reçoit plus de BPDUs. Le temps de forwarding de 15 secondes par défaut est le temps de passage d'un état "listening" à "learning" et de "learning" à "forwarding". Aussi, la fréquence d'envoi de BPDUs Hello est de 2 secondes par défaut.

Etat « Blocking » Bloqué

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- N'intègre aucun emplacement de station dans sa table MAC (il n'y pas d'apprentissage)
- Reçoit les BPDUs et les transmet à son système
- N'envoie pas de BPDUs reçus de son système
- Répond à SNMP

Etat « Listening » Ecoute

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- N'intègre aucune emplacement de station dans sa MAC table (il n'y pas d'apprentissage)
- Reçoit les BPDUs et les transmet à son système
- **Envoie les BPDUs reçus de son système**
- Répond à SNMP

Etat « Learning » Apprentissage

- Rejette toutes les trames de données venant du segment attaché
- Rejette toutes les trames de données venant d'un autre port de transfert
- **Intègre les emplacements de station dans sa table MAC (apprentissage)**
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

Etat « Forwarding » Acheminement

- **Commute toutes les trames de données venant du segment attaché**
- **Commute toutes les trames de données venant d'un autre port de transfert**
- Intègre les emplacements de station dans sa table MAC (apprentissage)
- Reçoit les BPDUs et les transmet à son système
- Envoie les BPDUs reçus de son système
- Répond à SNMP

Etat « Disabled » Inactif

- Cet état est similaire à l'état « blocking » sauf que le port est considéré physiquement non opérationnel (*shut down ou problème physique*).

IV. QUELQUES COMMANDES

Pour le diagnostic :

#**show spanning-tree**

Désactivation de STP :

(config)#**no spanning-tree vlan** *vlan-id*

Ports Portfast :

La configuration d'une interface en "Portfast" (passage directe de l'état "blocking" à l'état "forwarding" uniquement pour les segments qui ne connectent pas de switches) :

(config-if)#**spanning-tree portfast**

Priorité du switch :

(config)#**spanning-tree [vlan** *vlan-id*] **priority** *priority*

Coût et priorité d'un port :

(config-if)#**spanning-tree [vlan** *vlan-id*] **cost** *cost*
(config-if)#**spanning-tree [vlan** *vlan-id*] **port-priority** *priority*

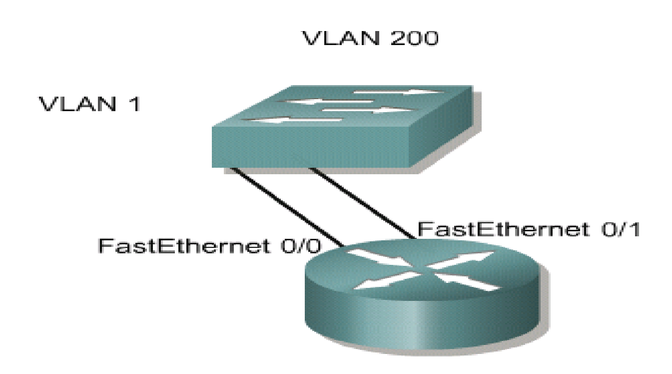
Paramètres de timing :

(config)#**spanning-tree [vlan** *vlan-id*] **max-age** *seconds*
6 à 200 secondes
(config)#**spanning-tree [vlan** *vlan-id*] **forward-time** *seconds*
4 à 200 secondes
(config)#**spanning-tree [vlan** *vlan-id*] **hello-time** *seconds*
1 à 10 secondes

F. Routage entre réseaux locaux virtuels.

I. Introduction au routage entre VLAN

Lorsqu'un hôte d'un domaine de broadcast souhaite communiquer avec un hôte d'un autre domaine de broadcast, un routeur doit être utilisé.

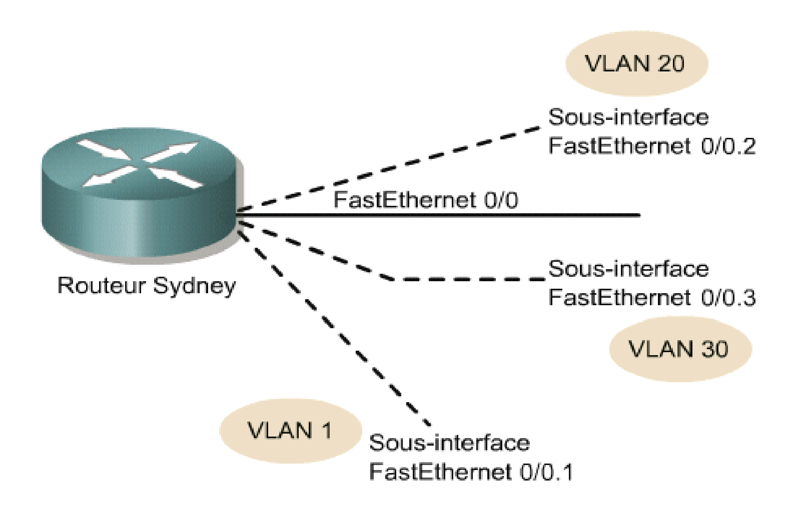


Un routeur doit être utilisé pour que les hôtes des différents VLAN communiquent.

Lorsqu'un VLAN s'étend sur plusieurs équipements, une agrégation est utilisée pour interconnecter les équipements. L'agrégation transporte le trafic de plusieurs VLAN. Par exemple, une agrégation peut connecter un commutateur à un autre commutateur, au routeur entre les VLAN ou à un serveur avec une carte NIC spéciale utilisée pour prendre en charge les agrégations.

II. Séparation des interfaces physiques en sous-interfaces

Une sous-interface est une interface logique au sein d'une interface physique, telle que l'interface Fast Ethernet d'un routeur.



Plusieurs sous-interfaces peuvent coexister sur une seule interface physique.

Chaque sous-interface prend en charge un VLAN et dispose d'une adresse IP affectée. Pour que plusieurs unités d'un même VLAN communiquent, les adresses IP de toutes les sous-interfaces maillées doivent être sur le même réseau ou sous-réseau. Par exemple, si la sous-interface FastEthernet 0/0.1 a l'adresse IP 192.168.1.1, alors 192.168.1.2, 192.168.1.3 et 192.1.1.4 sont les adresses IP des unités connectées à la sous-interface FastEthernet0/0.1.

Pour le routage entre VLAN avec sous-interfaces, une sous-interface doit être créée pour chaque VLAN.

```
Sydney(config)#interface FastEthernet 0/0.1
Sydney(config-subif)#description Administration VLAN1
Sydney(config)#interface FastEthernet 0/0.2
Sydney(config-subif)#description Comptabilite VLAN 20
Sydney(config)#interface FastEthernet 0/0.3
Sydney(config-subif)#description Ventes VLAN 30
```

La section suivante évoque les commandes nécessaires à la création de sous-interfaces et à l'application d'un protocole d'agrégation et d'une adresse IP à chaque sous-interface.

III. Configuration du routage entre des VLAN

Sur un routeur, une interface peut être logiquement divisée en plusieurs sous-interfaces virtuelles. Les sous-interfaces fournissent une solution flexible pour le routage de plusieurs flux de données via une interface physique unique. Pour définir des sous-interfaces sur une interface physique, effectuez les tâches suivantes:

- Identifiez l'interface.
- Définissez l'encapsulation VLAN.
- Attribuez une adresse IP à l'interface.

Pour identifier l'interface, utilisez la commande **interface** en mode de configuration globale.

Router(config)#**interface fastethernet** *numéro-port***.***numéro-sous-interface*

La variable *numéro-port* identifie l'interface physique tandis que la variable *numéro-sous-interface* identifie l'interface virtuelle.

Le routeur doit être capable de communiquer avec le commutateur à l'aide d'un protocole d'agrégation standardisé. Cela signifie que les deux unités interconnectées doivent se comprendre mutuellement. Dans l'exemple, 802.1Q est utilisé. Pour définir l'encapsulation VLAN, saisissez la commande **encapsulation** en mode de configuration d'interface.

Router(config-subif)#**encapsulation dot1Q** *numéro-vlan*

La variable *numéro-vlan* identifie le VLAN pour lequel la sous-interface achemine le trafic. Un ID de VLAN est ajouté à la trame uniquement lorsque celle-ci est destinée à un réseau non local. Chaque paquet VLAN transporte l'ID du VLAN dans son en-tête.

Pour affecter l'adresse IP à la sous-interface, entrez la commande suivante en mode de configuration d'interface.

Router(config-subif)#**ip address** *adresse-ip masque-sous-réseau*

G. Concepts et configuration de base d'un réseau sans fil.

I. Comparaison entre réseau local sans fil et un réseau local filaire

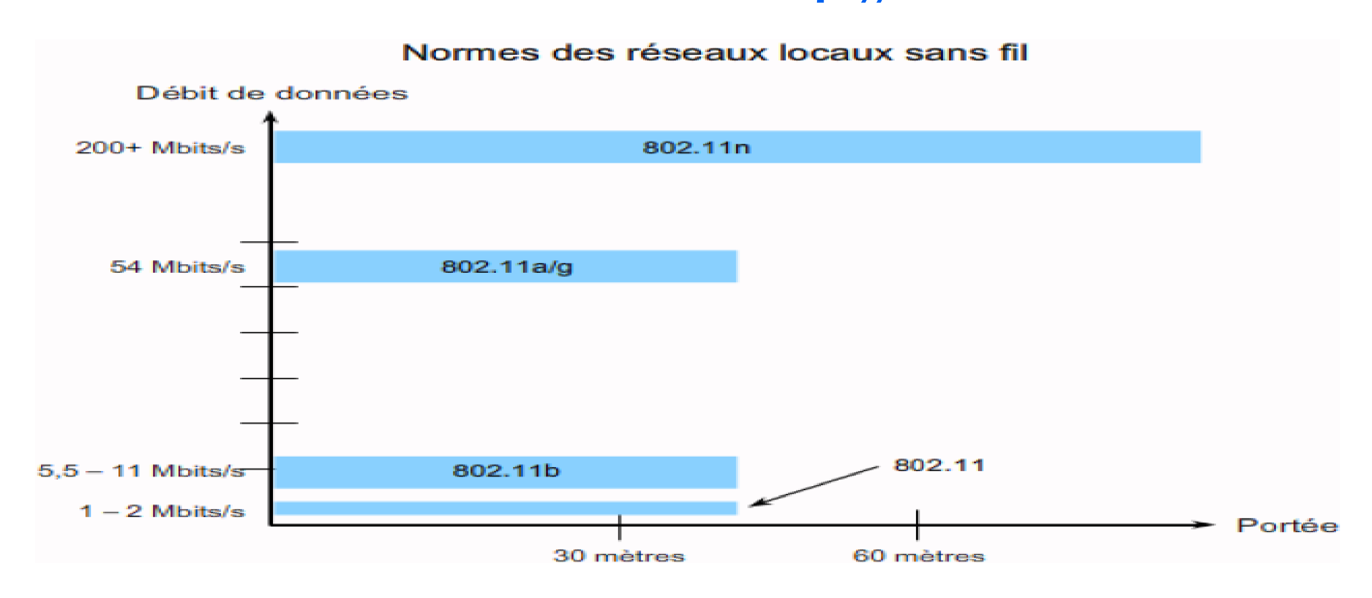
Les réseaux locaux sans fil et les réseaux locaux Ethernet ont la même origine. L'IEEE a adopté l'ensemble de normes d'architecture de réseau informatique 802 LAN/MAN. Les deux principaux groupes de travail 802 sont ceux du réseau local Ethernet 802.3 et du réseau local sans fil IEEE 802.11. Toutefois, il existe des différences importantes entre les deux.
Les réseaux locaux sans fil utilisent des radiofréquences (RF) et non des câbles au niveau de la couche physique et de la sous-couche MAC de la couche liaison de données. Par rapport au câble, les radiofréquences présentent les caractéristiques suivantes :

- Contrairement aux fils gainés, les radiofréquences n'ont pas de limites. Du fait de cette absence de limites, les trames de données peuvent être exploitées par quiconque pouvant recevoir le signal RF.
- Les radiofréquences ne sont pas protégées des signaux extérieurs. Autrement dit, les radios fonctionnant de manière indépendante sur un même secteur géographique mais qui utilisent des radiofréquences identiques ou similaires peuvent interférer entre elles.
- La transmission RF est soumise aux difficultés liées aux technologies reposant sur les ondes, comme les radios grands publics. Par exemple, à mesure que vous vous éloignez de la source, vous pouvez entendre plusieurs stations se chevaucher ou bien des chuchotements au niveau de la transmission. Vous pouvez même finir par perdre tout signal.
- La réglementation concernant les bandes RF peut être différente d'un pays à un autre.
- L'utilisation de réseaux locaux sans fil est soumise à d'autres réglementations et ensembles de normes qui ne s'appliquent pas aux réseaux locaux filaires.
- Dans un environnement de réseau local sans fil, les clients sont connectés au réseau par le biais non pas d'un commutateur Ethernet mais d'un point d'accès sans fil.
- Les réseaux locaux sans fil prennent en charge les hôtes qui rivalisent pour accéder aux supports RF (bandes de fréquences). L'ensemble de normes 802.11 prescrit l'évitement de collision plutôt que la détection de collision pour l'accès aux supports de façon à éviter par anticipation les collisions à l'intérieur des supports.
- Les réseaux locaux sans fil utilisent un format de trame différent de celui des réseaux locaux Ethernet filaires. Les réseaux locaux sans fil ont besoin d'informations supplémentaires au niveau de l'en-tête de couche 2 de la trame.
- Les réseaux locaux sans fil posent davantage de problèmes en matière de confidentialité dans la mesure où les fréquences radio peuvent atteindre l'extérieur.

Caractéristique	Réseau local sans fil 802.11	Réseaux locaux Ethernet 802.3
Couche physique	Radiofréquence (RF)	Câble
Accès aux supports	Évitement de collision	Détection de collisions
Disponibilité	Quiconque équipé d'une carte réseau radio dans la portée d'émission d'un point d'accès	Connexion par câble requise
Signaux parasites	Oui	Sans conséquence
Réglementation	Autres réglementations édictées par les autorités locales	Norme IEEE

II. Normes des réseaux locaux sans fil

La norme 802.11 relative aux réseaux locaux sans fil est une norme IEEE qui définit la façon dont les radiofréquences (RF) dans les bandes de fréquences 900 MHz, 2,4 GHz et 5 GHz appelées des bandes ISM (industrielles, scientifiques et médicales) sans licence sont utilisées pour la couche physique et la sous-couche MAC des liaisons sans fil.
Les normes relatives aux réseaux locaux sans fil se sont constamment améliorées avec la publication des normes IEEE 802.11a, IEEE 802.11b, IEEE 802.11g et 802.11n.



Normes des réseaux locaux sans fil

	802.11a	802.11b	802.11g		802.11n
Bande	5,7 GHz	2,4 GHz	2,4 GHz		2,4 et 5 GHz
Canaux*	Jusqu'à 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Débits de données	Jusqu'à 54 Mbits/s	Jusqu'à 11 Mbits/s	Jusqu'à 11 Mbits/s	Jusqu'à 54 Mbits/s	248 Mbits/s supposés pour deux flux MIMO
Avantages	~35 mètres Rapidité, moins sujette aux interférences	~35 mètres Faible coût, bonne portée	~35 mètres Rapidité, bonne portée, peu sensible aux obstacles		~70 mètres Excellents débits de données, portée accrue
Inconvénients	Coût plus élevé, portée inférieure	Lenteur, sujette aux interférences	Sujette aux interférences des appareils utilisant la bande 2,4 GHz		

III. Composants d'une infrastructure sans fil

3.1. Carte réseau sans fil

Un réseau local sans fil est constitué pour l'essentiel de stations clientes qui se connectent à des points d'accès qui, à leur tour, se connectent à l'infrastructure réseau. Le périphérique qui permet à une station cliente d'envoyer et recevoir des signaux RF est la carte réseau sans fil.

- À l'instar d'une carte réseau Ethernet, la carte réseau sans fil code un flux de données sur un signal RF selon la technique de modulation définie.
- À la différence des interfaces Ethernet 802.3 intégrées aux PC, la carte réseau sans fil n'est pas visible puisqu'il n'est pas nécessaire d'y connecter un câble.

3.2. Point d'accès sans fil :

Un point d'accès permet de relier des clients sans fil (ou stations) à un réseau local filaire. En règle générale, les périphériques clients ne communiquent pas directement entre eux ; ils communiquent avec le point d'accès.
Un point d'accès convertit les paquets de données TCP/IP en les faisant passer de leur format d'encapsulation de trames radio 802.11 au format de trame Ethernet 802.3 sur le réseau Ethernet filaire.
Dans un réseau d'infrastructure, les clients doivent être associés à un point d'accès pour pouvoir bénéficier de services réseau. Pour un client, l'association est le processus qui consiste à se joindre à un réseau 802.11.
Un point d'accès est un périphérique de couche 2 qui fonctionne comme un concentrateur Ethernet 802.3. Les radiofréquences constituent un support partagé et les points d'accès sont à l'écoute de l'ensemble du trafic radio. À l'image des périphériques Ethernet 802.3, les périphériques qui souhaitent utiliser le support se font concurrence. Toutefois, contrairement aux cartes réseau Ethernet, il est coûteux de fabriquer des cartes réseau sans fil qui puissent à la fois transmettre et recevoir des données, si bien que les périphériques radio ne détectent pas les collisions. Au lieu de cela, les périphériques wifi sont conçus pour les éviter.
Les points d'accès supervisent une fonction de coordination répartie appelée CSMA/CA (accès multiple avec écoute de porteuse avec évitement de collision). Cela veut simplement dire que les périphériques d'un réseau local sans fil doivent capter l'énergie au niveau du support (stimulation par radiofréquence au-dessus d'un certain seuil) et attendre que le support soit disponible avant de procéder à l'envoi.
On imagine le cas de deux stations clientes qui se connectent toutes deux à un même point d'accès, mais qui se trouvent de part et d'autre de celui-ci. Si la distance qui les sépare du point d'accès correspond à la portée maximale, elles ne pourront pas s'atteindre mutuellement. Autrement dit, ni l'une ni l'autre des deux stations ne captera l'autre sur le support, et elles risquent en fin de compte de transmettre simultanément. C'est ce que l'on appelle le problème du nœud (ou station) caché.

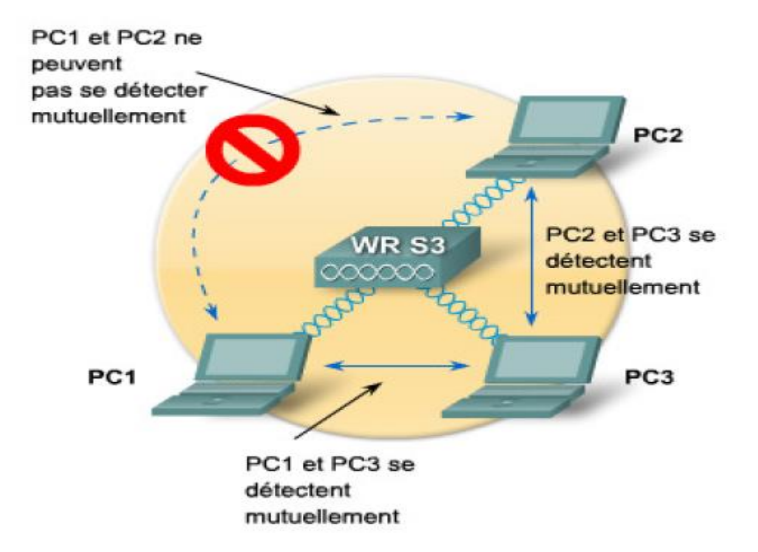
Un moyen de résoudre le problème du nœud caché est de recourir à une fonction CSMA/CA appelée Demande pour émettre/Prêt à émettre (DPE/PAE). La fonction DPE/PAE a été développée afin de permettre une négociation entre un client et un point d'accès. Lorsque la fonction DPE/PAE est activée dans un réseau, les points d'accès affectent le support à la station demandeuse le temps qu'il faut pour terminer la transmission. Lorsque la transmission est terminée, les autres stations peuvent demander le canal de la même façon. Sinon, la fonction normale d'évitement de collision est rétablie.

Points d'accès sans fil

Problème du nœud caché :

- PC1 et PC2 accèdent à S3
- PC1 et PC2 ne peuvent pas s'atteindre mutuellement
- PC1 ne détecte pas l'activité de PC2 sur le canal
- PC1 envoie des données pendant que PC2 en transmet
- Une collision se produit

PC3 étant détecté à la fois par PC1 et PC2, aucune collision n'implique PC3.



3.3. Routeur sans fil :

Les routeurs sans fil jouent le rôle de point d'accès, de commutateur Ethernet et de routeur. Par exemple, le périphérique Linksys WRT300N est un appareil « trois en un ». Il se compose tout d'abord d'un point d'accès sans fil, qui assure les fonctions classiques d'un point d'accès ; ensuite, d'un commutateur intégré 10/100 bidirectionnel simultané à quatre ports, qui fournit une connectivité aux périphériques filaires ; et enfin, d'une fonction de routeur, qui procure une passerelle pour se connecter aux autres infrastructures réseau.

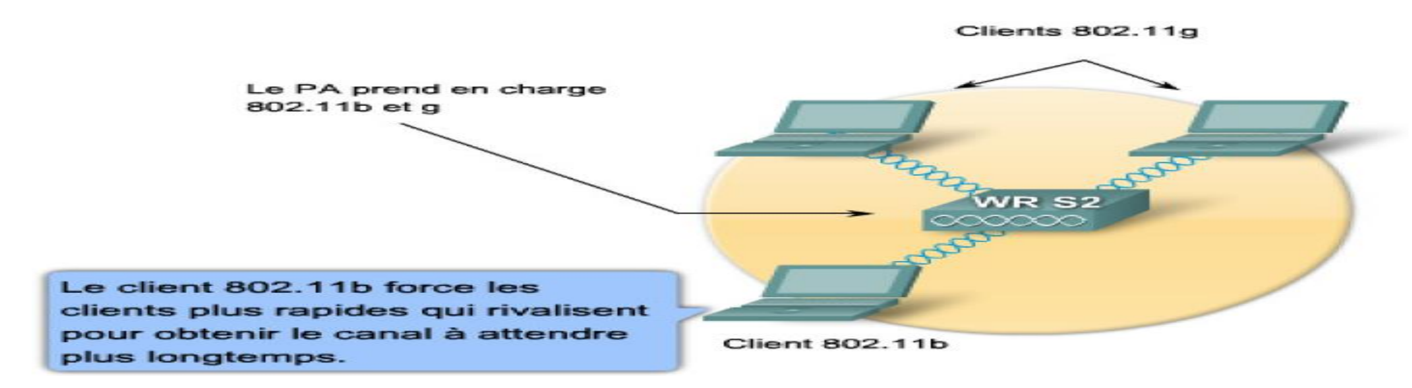
IV. Paramètres configurables pour le fonctionnement des réseaux sans fil

La figure présente l'écran initial de configuration sans fil d'un routeur sans fil Linksys. La création d'une connexion entre un client et un point d'accès implique plusieurs processus. On doit configurer les paramètres sur le point d'accès (et par la suite sur votre périphérique client) pour permettre la négociation de ces processus.



4.1. Mode réseau sans fil

Le paramètre Wireless Network Mode (Mode réseau sans fil) fait référence aux protocoles de réseau local sans fil suivants : 802.11a, b, g ou n. Le protocole 802.11g étant compatible en amont avec 802.11b, les points d'accès prennent en charge les deux normes. Il ne faut pas perdre de vue que si tous les clients se connectent à un point d'accès conformément à la norme 802.11g, ils bénéficient tous des meilleurs débits de données disponibles. Lorsque des clients 802.11b s'associent au point d'accès, tous les clients rapides qui rivalisent pour obtenir le canal doivent attendre que les clients 802.11b aient libéré le canal avant de transmettre. Lorsqu'un point d'accès Linksys est configuré pour autoriser les clients 802.11b et 802.11g, il fonctionne en mode mixte.



Pour permettre à un point d'accès de prendre en charge 802.11a, ainsi que 802.11b et g, il doit disposer d'une seconde radio pour fonctionner dans l'autre bande RF.

4.2. SSID : Service Set Identifier

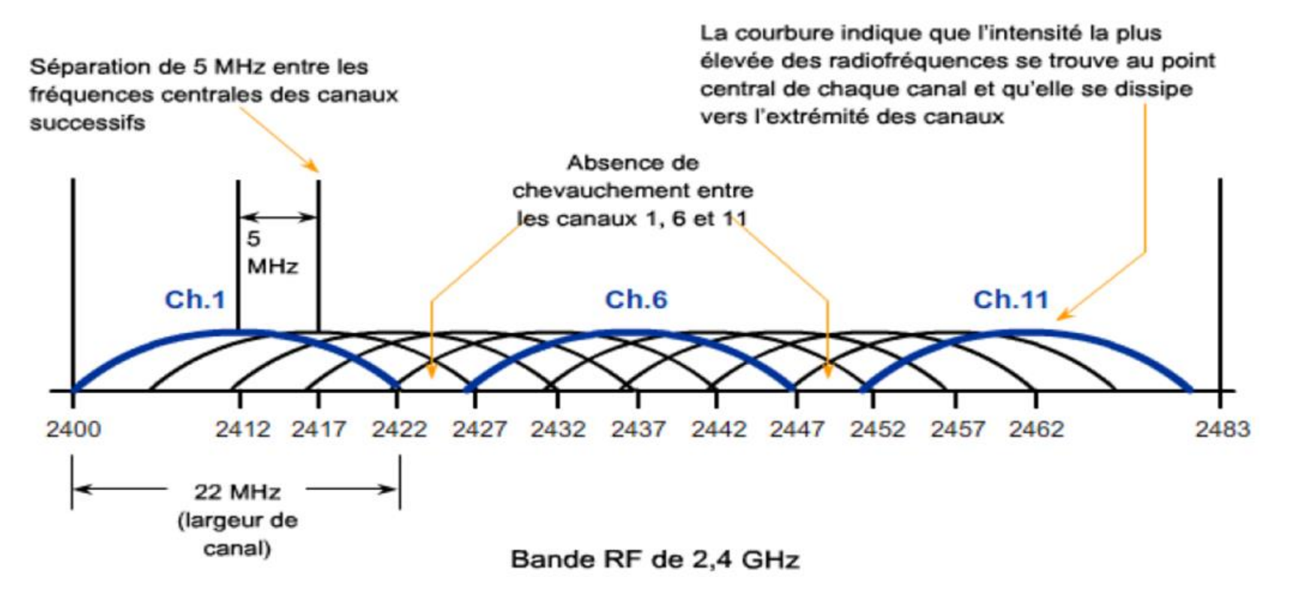
Un identificateur d'ensemble de services partagé SSID est un identificateur unique qu'utilisent les périphériques client pour distinguer plusieurs réseaux sans fil dans un même voisinage. La figure illustre un exemple de SSID permettant de distinguer plusieurs réseaux locaux sans fil. Les SSID peuvent correspondre à une entrée alphanumérique, sensible à la casse, constituée de 2 à 32 caractères.



4.3. Canaux des bandes RF

La norme IEEE 802.11 établit le modèle de découpage en canaux pour l'utilisation des bandes RF ISM sans licence dans les réseaux locaux sans fil. La bande 2,4 GHz est découpée en 11 canaux pour l'Amérique du Nord et en 13 canaux pour l'Europe. La fréquence centrale de ces canaux est séparée de seulement 5 MHz et leur bande passante globale (ou occupation de fréquence) est de 22 MHz.

Une bande passante de canal de 22 MHz combinée à une séparation de 5 MHz entre les fréquences centrales signifie qu'il existe un chevauchement entre les canaux successifs. Or, dans le cas des réseaux locaux sans fil qui nécessitent plusieurs points d'accès, les Méthodes Recommandées préconisent l'utilisation de canaux sans chevauchement. S'il existe trois points d'accès adjacents, utilisez les canaux 1, 6 et 11. S'il n'en existe que deux, sélectionnez-en deux qui soient séparés de cinq canaux (p. ex., les canaux 5 et 10). Bon nombre de points d'accès sont en mesure de sélectionner automatiquement un canal en fonction de l'utilisation de canaux adjacents. Certains produits surveillent constamment l'espace radio pour ajuster dynamiquement les paramètres des canaux en réponse aux changements intervenant dans l'environnement.

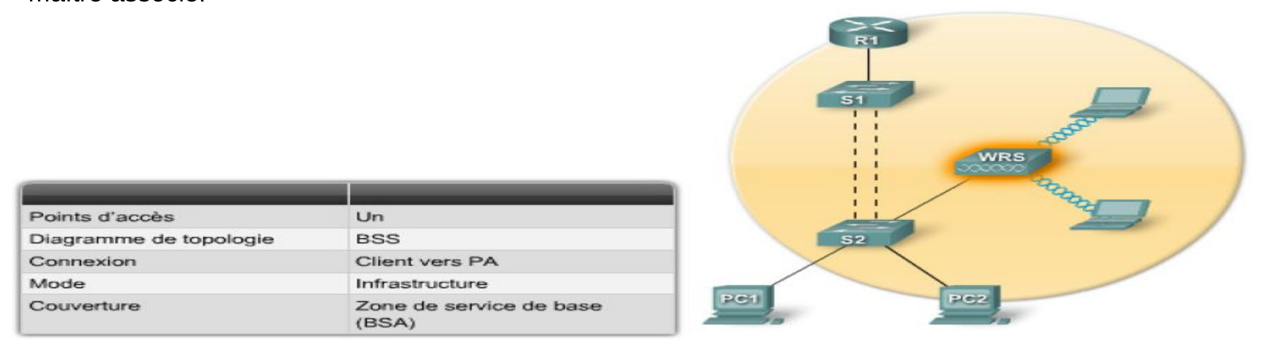


4.4. Topologie 802.11

Lorsque deux cartes sans fil sont configurées pour employer le même protocole sur le même canal radio, alors elles peuvent négocier la connectivité de la couche liaison de données. Chaque dispositif 802.11a/b/g/n peut fonctionner dans un des quatre modes possibles suivants:

a) Le ***mode maître*** (aussi nommé ***AP*** ou ***mode infrastructure***) est employé pour créer un service qui ressemble à un point d'accès traditionnel. La carte sans fil crée un réseau avec un canal et un nom spécifique (appelé le ***SSID***) pour offrir ses services. Sur ce mode, les cartes sans fil contrôlent toutes les communications liées au réseau (authentification des clients sans fil, contrôle d'accès au canal, répétition de paquets, etc...) Les cartes sans fil en mode maître peuvent seulement communiquer avec les cartes qui sont associées à lui en mode administré.

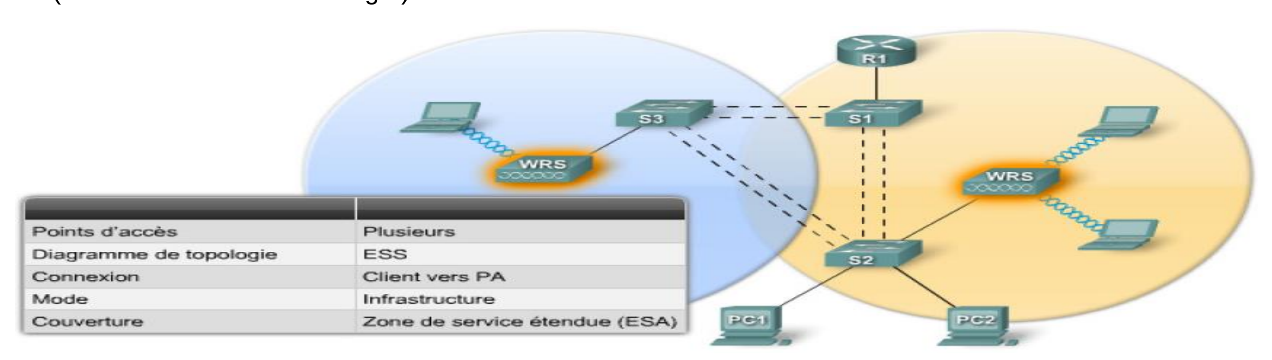
b) Le ***mode administré*** (managed mode en anglais) est également parfois désigné sous le nom de mode client. Les cartes sans fil en mode administré joindront un réseau créé par un maître et changeront automatiquement leur canal pour que celui-ci corresponde à celui du maître. Ensuite, elles présentent leurs identifications au maître. Si celles-ci sont acceptées, elles sont alors associées au maître. Les cartes en mode administré ne communiquent pas entre-elles directement et communiqueront uniquement avec un maître associé.



Points d'accès	Un
Diagramme de topologie	BSS
Connexion	Client vers PA
Mode	Infrastructure
Couverture	Zone de service de base (BSA)

Lorsqu'un ensemble de services de base n'assure pas une couverture en radiofréquences suffisante, un ou plusieurs ensembles de ce type peuvent être joints par le biais d'un système de distribution commun de manière à former un éventail de services étendu (ESS). Dans un ESS, un BSS se distingue d'un autre par son identificateur (BSSID), qui correspond à l'adresse MAC du point d'accès desservant le BSS. La zone de couverture est la zone de services étendue (Extended Service Area, ESA).

Le système de distribution commun permet à plusieurs points d'accès au sein d'un ensemble de services étendus d'apparaître en tant qu'ensemble de services de base unique. En règle générale, un ensemble de services étendus comprend un SSID commun qui permet à un utilisateur de passer d'un point d'accès à un autre (« itinérance » ou « roaming »).



Points d'accès	Plusieurs
Diagramme de topologie	ESS
Connexion	Client vers PA
Mode	Infrastructure
Couverture	Zone de service étendue (ESA)

c) Le ***mode ad hoc*** crée un réseau multipoint à multipoint où il n'y a aucun nœud maître ou AP. En mode ad hoc, chaque carte sans fil communique directement avec ses voisins. Les nœuds doivent être à la portée des autres pour communiquer, et doivent convenir d'un nom de réseau et un canal.



Points d'accès	Aucun
Diagramme de topologie	IBSS
Connexion	Peer to peer
Mode	Ad hoc
Couverture	Zone de service de base (BSA)

d) Le ***mode moniteur*** est employé par certains outils (tels que Kismet) pour écouter passivement tout le trafic radio sur un canal donné. Lorsqu'elles se trouvent en mode moniteur, les cartes sans fil ne transmettent aucune donnée. Ceci est utile pour analyser des problèmes sur un lien sans fil ou observer l'utilisation de spectre dans le secteur local. Le mode moniteur n'est pas utilisé pour des communications normales.

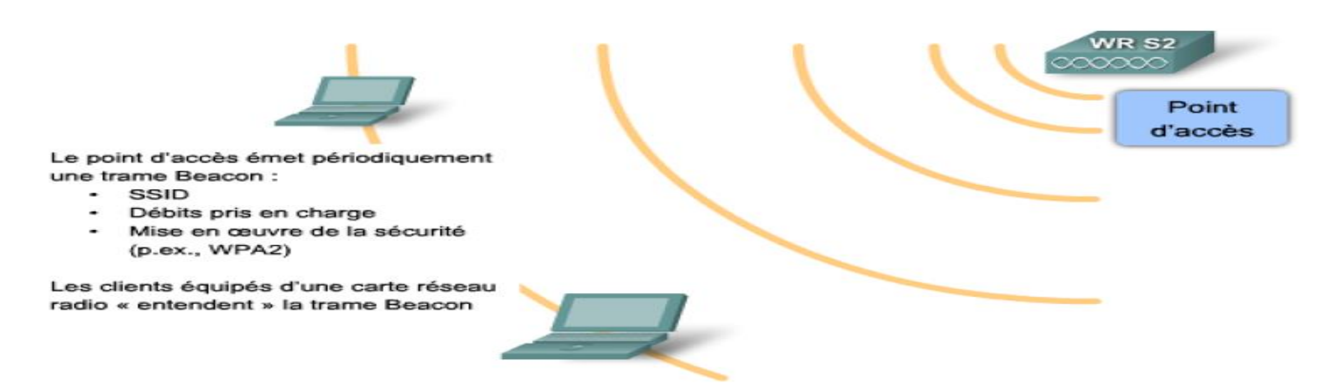
Récapitulatif des topologies de réseau LAN sans fil

Périphériques sans fil	Mode Topologie	Base de la topologie	Zone de couverture
Aucun point d'accès	Ad hoc	Ensemble de services de base indépendants (IBSS)	Zone de service de base (BSA)
Un point d'accès	Infrastructure	Ensemble de services de base (BSS)	Zone de service de base (BSA)
Plusieurs points d'accès	Infrastructure	Ensemble de services étendus (ESS)	Zone de service étendue (ESA)

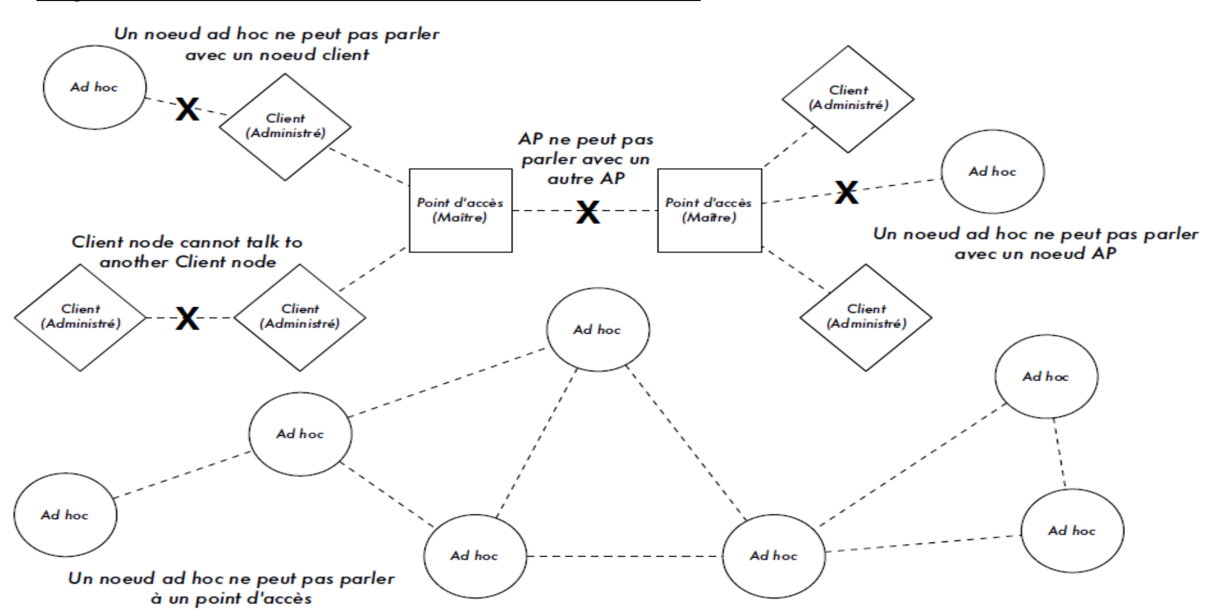
4.5. Association du client au point d'accès

L'une des principales étapes du processus 802.11 est celle qui consiste à découvrir un réseau local sans fil et ensuite à s'y connecter. Les principales composantes de ce processus sont les suivantes :

- Trames Beacon - Trames de diffusion émise par le point d'accès pour annoncer sa présence.
- Analyseurs - Trames utilisées par les clients des réseaux locaux sans fil pour trouver leur réseau.
- Authentification - Processus correspondant à un objet représentatif de la norme 802.11 d'origine mais qui reste exigé par la norme.
- Association - Processus visant à établir une liaison de données entre un point d'accès et un client de réseau local sans fil.



4.1. Règles d'association entre AP, Clients et nœuds Ad Hoc.



Lorsque nous réalisons une liaison point à point ou point à multipoint, une radio fonctionnera typiquement en mode maître, alors que l'autre (ou les autres) fonctionnera en mode réseau.
Dans un réseau maillé multipoint à multipoint, toutes les radios fonctionnent en mode ad hoc de sorte qu'elles puissent communiquer les unes avec les autres directement.

V. Protocoles de sécurité sans fil

5.1. Vue d'ensemble des protocoles sans fil :

Le Wired Equivalent Privacy (abrégé WEP) est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.
Cependant, plusieurs faiblesses graves ont été identifiées par les cryptologues. Le WEP est parfois surnommé Weak Encryption Protocol (faible protocole de cryptage). Le WEP a donc été supplanté par le WPA (Wi-Fi Protected Access) en 2003, puis par le WPA2 en 2004 (WPA2 est la version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance).

5.2. WEP (Wired Equivalent Privacy)

Le WEP utilise l'algorithme de chiffrement par flot RC4 (Rivest Cipher 4) pour assurer la confidentialité et la somme de contrôle CRC-32 pour assurer l'intégrité.
Le WEP 64 bits utilise une clé de chiffrement de 40 bits à laquelle est concaténé un vecteur d'initialisation (initialization vector ou IV en anglais) de 24 bits. La clé et le vecteur d'initialisation forment ainsi une clé RC4 de 64 bits permettant de chiffrer les données échangées.
Une clé WEP de 128 bits est saisie comme une suite de 13 caractères ASCII ou 26 caractères hexadécimaux. Chaque doublet hexadécimal représente 8 bits de la clé WEP. 8 * 13 = 104 bits. En ajoutant le vecteur d'initialisation (IV) de 24 bits, on obtient ce que l'on appelle « une clé WEP de 128 bits ».
Un mécanisme utilisant des clés WEP de 256 bits est disponible. Comme pour les mécanismes précédemment mentionnés, 24 bits sont réservés pour le vecteur d'initialisation (IV), laissant ainsi 232 bits pour la clé de chiffrement. Cette clé est habituellement saisie comme une suite de 58 symboles hexadécimaux. (58 * 4 = 232 bits) + 24 = 256 bits.
Malheureusement, la longueur des clés n'est pas le problème de sécurité le plus sévère du WEP.

5.3. WPA et WPA2 (Wi-Fi Protected Access)

- Selon la version :
  - WPA : la version initiale améliore la sécurité offerte par l'ancien protocole WEP. WPA utilise en général le protocole de chiffrement TKIP (voir plus loin).
  - WPA2 : également connu sous le nom IEEE 802.11i-2004, ce successeur de WPA remplace le chiffrement TKIP par AES pour plus de sécurité. La compatibilité WPA2 est obligatoire pour les équipements certifiées Wi-Fi depuis 2006.

- Selon le groupe d'utilisateurs visés :
  - WPA personnel (WPA-Personal) : connu également sous le nom de mode à secret partagé ou WPA-PSK (Pre-shared key), WPA personnel est conçu pour les réseaux personnels ou de petites entreprises, car il n'y a pas besoin d'utiliser un serveur d'authentification. Chaque équipement du réseau sans fil s'authentifie auprès du point d'accès en utilisant la même clé sur 256 bits.
  - WPA entreprise (WPA-Enterprise) : connu également sous le nom de mode WPA-802.1X ou WPA-EAP(Extensible Authentication Protocol), WPA entreprise est conçu pour les réseaux d'entreprise et demande à ce que l'on installe un serveur d'authentification RADIUS. C'est plus compliqué à mettre en place, mais offre plus de sécurité. Le protocole EAP utilisé pour l'authentification existe en plusieurs variantes, dont EAP-TLS, EAP-TTLS et EAP-SIM.

  Remarque : WPA personnel et WPA entreprise concernent à la fois WPA et WPA2.

- Selon le protocole de chiffrement :
  - TKIP (Temporal Key Integrity Protocol) : une clé de 128 bits est utilisée pour chaque paquet. On génère une nouvelle clé pour chaque paquet.
  - AES (Advanced Encryption Standard) qui est plus fort que TKIP.

TKIP – Temporal Key Integrity Key	AES – Advanced Encryption Standard
• Chiffrement par l'ajout de codage de bits de plus en plus complexe à chaque paquet • Basé sur le même algorithme de chiffrement (RC4) que WEP	• Nouvel algorithme de chiffrement utilisé dans 802.11i • Basé sur TKIP avec des fonctionnalités supplémentaires qui améliorent le niveau de sécurité offert

Même si TKIP pallie toutes les faiblesses connues de WEP, le chiffrement AES de WPA2 est la méthode à privilégier, car elle met les normes de chiffrement applicables aux réseaux locaux sans fil en phase avec les méthodes recommandées et des normes plus générales de l'industrie informatique, plus particulièrement la norme IEEE 802.11i.

Lorsque l'on configure des points d'accès ou des routeurs sans fil Linksys, tels que le modèle WRT300N, il se peut que WPA ou WPA2 n'apparaissent pas, mais qu'il soit en revanche fait mention de ce que l'on appelle une clé pré-partagée (PSK). Il existe différents types de PSK, à savoir :

- PSK ou PSK2 couplé à TKIP est l'équivalent de WPA
- PSK ou PSK2 couplé à AES est l'équivalent de WPA2
- PSK2, sans méthode de chiffrement spécifiée, est l'équivalent de WPA2

5.4. Récapitulatif

Principales étapes de sécurisation des réseaux locaux sans fil

Accès ouvert	Chiffrement de première génération	Provisoire	Présent
SSID	WEP	WPA	802.11i/WPA2
• Aucun chiffrement • Authentification de base • N'est pas un dispositif de sécurité	• Authentification non efficace • Clés statiques, cassables • Non évolutif	• Standardisé • Chiffrement amélioré • Authentification utilisateur efficace (p.ex., LEAP, PEAP, EAP-FAST)	• Chiffrement AES • Authentification : 802.1X • Gestion des clés dynamiques • WPA2 correspond à la mise en œuvre de la norme 802.11i par la Wi-Fi Alliance